Information Technology Support Services (ITSS)
Performance Work Statement

CONTRACT NUMBER: GSQ0915BH0020 / Task Order ID09150006

Contractor:

Federal Acquisition Services Alliant Joint Venture, LLC (FASA)
16901 Melford Blvd, Suite 101
Bowie, MD 20715
DUNS: 788625429

Defense Manpower Data Center (DMDC)
Systems and Technical Support Division
400 Gigling Road
Seaside, CA 93955

GSA, FAS, Pacific Rim Region
Acquisition Operations Division
50 United Nations Plaza
San Francisco, CA 94102

Period of Performance: Six (6) Month Base Period and nine (9) six (6) Month Option Periods as follows:

Base Period: 08/10/2015 – 02/09/2016
Option Period 1: 02/10/2016 – 08/09/2016
Option Period 2: 08/10/2016 – 02/09/2017
Option Period 3: 02/10/2017 – 08/09/2017
Option Period 4: 08/10/2017 – 02/09/2018
Option Period 5: 02/10/2018 – 08/09/2018
Option Period 6: 08/10/2018 – 02/09/2019
Option Period 7: 02/10/2019 – 08/09/2019
Option Period 8: 08/10/2019 – 02/09/2020
Option Period 9: 02/10/2020 – 08/09/2020

MODIFICATIONS:

This Performance Work Statement (PWS), along with FASA's Technical Proposal dated 09 July 2015 are hereby incorporated into the Task Order Award: GSQ0915BH0020 / Task Order ID09150006.

P0001 – This PWS, along with FASA's Technical and Price proposal dated 17 September 2015 are hereby incorporated into the Task Order Award: GSQ0915BH0020_P0001.

P0002 – This PWS, along with FASA's Technical and Price proposal dated 01 December 2015 are hereby incorporated into the Task Order Award: GSQ0915BH0020_P0002.

P0003 – This PWS, along with FASA's Technical and Price proposal dated 03 February 2016 are hereby incorporated into the Task Order Award : GSQ0915BH0020_P0003.

P0005 – This PWS, along with FASA's Technical and Price proposal dated 11 March 2016 are hereby incorporated into the Task Order Award: GSQ0915BH0020_P0005 with the condition that all FTE allocations will be re-evaluated for Option periods 2 - 9 , if those options will be exercised and if applicable, at the discretion of the Government.

P0006 – This PWS, along with FASA's Technical and price Proposal dated 07 June 2016 are hereby incorporated into the Task Order Award: GSQ0915BH0020_P0006 with the condition that all FTE allocations will be re-evaluated for Option Periods 2 -9, if those options will be exercised and if applicable, at the discretion of the Government.

P0007 – This PWS incorporates changes outlined in FASA revised Technical Proposal submitted on 14, June 2016 to CLIN 1001, 1002, 1004, 1005 and 1007 for Over and Above/Surge Requirements for the Defense Information System for Security (DISS) Support Services into Option Period 1. DISS

work under this modification has been separated into two support periods from the DISS project, Implementation (07/22/2016 -05/09/2017) and Sustainment (05/10/17 – 08/09/2017). The work required in Option Period 2 and Option Period 3, is subject to the Option Periods being exercised.

P0008 – The purpose of P0008 is to Exercise Option Period Two (2) of the task order in accordance with the PWS. Option Period Two (2) period of performance is 08/10/2016 – 02/09/2017.

P0009 – This PWS, along with FASA's Technical and Price proposal dated 12 September 2016 are hereby incorporated for additional support for JBOSS Development Environment and Defense Civilian Personnel Advisory Service (DCPAS) into the contract Performance Work Statement (PWS). Modification P0009 also incorporates additional Security Staffing to support the DMDC Security Posture (ATO Requirements) into the contract Performance Work Statement (PWS).

Additional Contract Clauses and Requirements:

1. FAR 52.217-5--Evaluation of Options (July 1990): Except when it is determined in accordance with FAR 17.206(b) not to be in the Government's best interests, the Government will evaluate offers for award purposes by adding the total price for all options to the total price for the basic requirement. Evaluation of options will not obligate the Government to exercise the option(s). (End of provision)

2. FAR 52.217-8--Option to Extend Services (Nov 1999): The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 5 calendar days. (End of Clause)

3. FAR 52.217-9--Option to Extend the Term of the Contract (Mar 2000): The Government may extend the term of this contract by written notice to the Contractor within 10 days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 30 days before the contract expires. The preliminary notice does not commit the Government to an extension. If the Government exercises this option, the extended contract shall be considered to include this option clause. The total duration of this contract, including the exercise of any options under this clause, shall not exceed 30 months. (End of Clause)

4. FAR 52.245-1 -- Government Property (Jun 2007)

5. FAR 52.219-14 Limitations on Subcontracting (NOV 2011)

6. FAR 52.219-13 Notice of Set-Aside of Orders (NOV 2011)

7. FAR 52.219-6 Notice of Total Small Business Set-Aside (NOV 2011)

8. FAR 52.227-14 Data Requirements (General)

9. FAR 52.227-16 Additional Rights in Data

10. DFAR 252.227-7013 Rights in Technical Data--Noncommercial Items.

11. DFAR 252.227-7014 Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation.

12. DFAR 252.227-7015 Technical Data–Commercial Items.

13. DFAR 252.227-7022 Government Rights (Unlimited).

14. GSAM 552.232-73, Availability of Funds (Sep 1999)

15. SOFTWARE MADE AVAILABLE FOR CONTRACTOR'S USE (May 2008)
    a) The Government, from time to time, may make certain software acquired under license available to the contractor for its use in the performance of this contract.
    b) The contractor recognizes and acknowledges that such software or data contained therein may be proprietary and confidential to a third party.
    c) The contractor agrees that it and its employees will not use, copy, disclose, modify, or reverse engineer such software except as permitted by the license and any other terms and conditions under which the software is made available to the contractor.
    d) The contractor is not authorized to violate any software licensing agreement, or to cause the Government to violate any licensing agreement. If, at any time during the performance of this contract, the contractor has reason to believe that its use of Government furnished software may involve or result in a violation of NSF's licensing agreement, the contractor shall promptly notify the CO, in writing, of the pertinent facts and circumstances. Pending direction from the CO, the contractor shall continue to perform to the full extent possible without using the software in question.

16. ORGANIZATIONAL CONFLICT OF INTEREST
    a) The contractor warrants that, to the best of the contractor's knowledge and belief, there are no relevant facts or circumstances which could give rise to an organizational conflict of interest, as defined in FAR Subpart 9.5, or that the contractor has disclosed all such relevant information.

    b) The contractor agrees that if an actual or potential organizational conflict of interest is discovered after award, the contractor will make a full disclosure in writing to the CO immediately. This disclosure shall include a description of actions which the contractor has taken or proposes to take, after consultation with the CO, to avoid, mitigate, or neutralize the actual or potential conflict.

c) Remedies - The Government may terminate this contract for convenience, in whole or in part, if it deems such termination necessary to avoid an organizational conflict of interest. If the contractor was aware of a potential organizational conflict of interest prior to award or discovered an actual or potential conflict after award and did not disclose or misrepresented relevant information to the CO, the Government may terminate the contract for default, or pursue such other remedies as may be permitted by law or this contract.

d) The contractor further agrees to insert in any subcontract or consultant agreement hereunder, provisions which shall conform substantially to the language of this clause, including this paragraph (d).

e) The contractor will be required to warrant that, to the best of its knowledge and belief, and except as otherwise set forth in this contract, it does not have any organizational conflict of interest as defined in FAR 2.101 and FAR Subpart 9.5.

f) Undisclosed Organizational Conflicts of Interest will be grounds for Termination for Default.

17. Optional Performance Periods (Service Renewals):
The Government may exercise Option Performance periods and Optional Services CLINs as identified in the reference pricing schedule. FASA must provide pricing data for all Optional performance requirements as identified in the PWS for Over and Above CLINs and Surge CLINs. All Optional CLINs may be exercised at the sole discretion of the Government and are contingent upon the availability of funds and changing technological requirements.

The Contractor shall provide all deliverables as stated in the Government Provided PWS, including the Quality Assurance Surveillance Plan (QASP), Monthly Progress Status Reports, Monthly Invoices and AQLs Identified.

TABLE OF CONTENTS

1.0 INTRODUCTION

Organization to be supported:
Defense Manpower Data Center (DMDC)
Systems and technical Support Division
400 Gigling Road
Seaside, CA 93955

The Defense Manpower Data Center (DMDC) requires support services and solutions that span the entire spectrum of existing and future technical environments, hardware and software systems, lifecycle and applications in support of both its Unclassified Non-secure Internet Protocol Router Network (**NIPRNET**) and Classified Secure Internet Protocol Router Network (**SIPRNET**) environments.

The General Services Administration (GSA), Pacific Rim Region is conducting this acquisition on the behalf of the Defense Manpower Data Center (DMDC). The contract type will be a mixed Firm Fixed Price (FFP) and Labor Hour task order. The contractor shall be responsible for providing all the necessary labor and services to accomplish the requirements in this PWS.

The Contractor shall be responsible for complying with all applicable Federal Acquisition Regulations (FAR), Defense Acquisition Regulations (DFAR) and General Services Administration Acquisition Manual (GSAM).

2.1 BACKGROUND / OVERVIEW

2.2 DMDC supports major programs and initiatives within the Department of Defense (DoD) and maintains the largest archive of personnel, manpower, training, security and financial data within the DoD. The personnel data holdings, in particular, are broad in scope and date back to the early 1970's, covering all Uniformed Services, all components of the Total Force (Active Duty, Guard, Reserve, and Civilian), and all phases of the personnel life cycle (accessions through separation/retirement). The categories of data archived at DMDC represent significant data holdings and, in most cases, provide the only single source of commonly coded data for the Uniformed Services. These data support decision-making by the Office of the Secretary of Defense for Personnel and Readiness (OUSD (P&R)), other Office of the Secretary of Defense (OSD) organizations, and a wide variety of customers both within and outside the DoD. DMDC's programs include verifying military entitlements and benefits; managing the DoD ID card issuance program; providing identity management for the DoD; helping identify fraud and waste in DoD pay and benefit systems; personnel and property identification; authentication, and access control systems; personnel evacuation support systems; conducting personnel surveys; and assisting military members and their spouses with relocations, quality of life issues and post-service job searches. DEERS application systems and supporting databases must be available to the user community 24 hours per day 7 days per week with sub-second response time. Any outage can result in disruption of services to DoD beneficiaries as well as potential financial claims from the TRICARE Next

Generation (TNEX) Contractors. Additional information about DMDC can be obtained at https://www.dmdc.osd.mil.

2.3 DMDC is a geographically dispersed separated organization with facilities both Contractor and Government located in Seaside, CA, Boyers, PA, DISA, Columbus, OH, Colorado Springs, CO, Fort Knox, KY and the National Capitol Region. DMDC also has support offices in Germany, the Republic of Korea, Qatar and Kuwait. The Director of DMDC is located at the Mark Center in Alexandria, VA.

2.4 Office of the Chief Information Office (CIO)

The work under this requirement falls under the auspices of the Office of the Chief Information Officer (CIO). The CIO is responsible for all DMDC Information Technology (IT) related functions, including the development of IT strategies, enterprise architecture, IT investment and portfolio management, and information assurance. The CIO has total system management responsibilities that include long-range planning, requirements definition, alternative analysis, design, acquisition or development, integration, testing, implementation, and ongoing operations, maintenance, and administration of both hardware and software.

2.3.1 Information Technology Operations Division (IT OPS)

Under the direction of the DMDC CIO, the Information Technology Operations (IT OPS) Division provides IT service management support for information systems located at DMDC enterprise sites, Department of Defense (DoD) consolidated data centers, and Government furnished equipment (GFE) located at off-site facilities. The mission is to provide the IT infrastructure which enables the business units to accomplish the DMDC Mission. The IT OPS Division provides a wide range of core infrastructure services out of multiple geographically distributed Data Centers, including Desktop/Client Services (including File & Print, COTS Applications and Software distribution, Remote Access and Terminal Services, Virtualized Desktop Services, Laptop and Mobile Device Management); Network Services (WAN, LAN, Extranet); Telephony Services (including VoIP, Data Convergence and Unified Messaging); Video Tele-Conferencing (VTC) support; Corporate Messaging and Directory Services; Authentication, PKI and Security Services; Storage and Backup Services, and Middleware Services for both SQL and Oracle Data Base architectures. All services are underpinned by a customer facing Service Desk organization which has full integration and harmonization with the CIO and IT OPS. These infrastructure services are complemented by Professional Services and Logistical Capabilities including a full range of Information Technology Infrastructure Library (ITIL) Process areas (Incident/Problem/Change/Configuration/IT Asset/Capacity/Service Level Management/Project Management and Governance). The IT Operations Division develops and assures compliance with policies, directives, plans, and procedures for the control and security of all system development and maintenance activities ensuring the confidentiality, integrity and availability of DMDCs systems.

3.0 SCOPE

3.1. The Contractor shall provide all necessary labor and services (non-personal), except as specified by the Government, required to support a full range of IT related services and technical

solutions that encompasses enterprise level system administration services, operations, Configuration Management , security management, testing, quality assurance and sustainment requirements of the DMDC installed infrastructure, as well as infrastructure design and deployment of new system initiatives as stated within the PWS. The contractor shall remain abreast of emerging technologies in the marketplace and recommend changes, modifications, and upgrades and industry best practices.

3.2 DMDC Information Technology Overview and Environment

3.2.1 The major components of DMDC's IT environment, major programs and COTS software supported by this PWS are described in the Appendices list found in section 15.0, DMDC anticipates that these components, applications and information may change before and during the performance of this effort.

3.2.2 The Contractor is required to comply with all applicable laws, policies, procedures, and apply federal Government best practices. The Contractor will ensure all Information Technology projects, applications, systems, programs, or other areas of support provided hereunder comply with, adhere to and are guided by the standard program inception, elaboration, construction, and maintenance application life cycle methodology (see DoD Architecture Framework (DoDAF) version 2.02,) see < http://dodcio.defense.gov/dodaf20.aspx

3.3 Objectives

The objective of this task order is to obtain Information Technology Support Services to support the DMDC program to include the following minimum requirements:

3.4 Expertise, Staffing and Certification

3.4.1 The Contractor shall provide personnel with expertise to successfully perform this task and maintain a training program to ensure their staff is adequately trained and current on required skills, certifications and qualifications. Personnel shall demonstrate good communication skills and shall be flexible and adaptable in a dynamic environment. The Contractor shall effectively participate in planning and strategy sessions, effectively interact with customers, resolve complaints and problems, and keep management properly informed as to operational issues, problems, future needs, and technological developments. In addition to the core competencies related to their jobs, ensure that the employees are trained on customer support protocols and customer relations. Reimbursement for training shall not be authorized for contractor employees. The Contractor shall have full responsibility for keeping their employees trained and abreast of advances in the standard commercial and network technologies implemented in the Agency.

3.4.2 The contractor shall ensure the certification compliance IAW DoD 8570.01-M Information Assurance Workforce Improvement Program. The contractor personnel shall agree as a "condition of employment" to obtain the appropriate baseline certifications upon contract award. The contractor shall ensure all employees meet the minimum requirements within six months of the task order award. Further, the contractor shall ensure all new employees meet the minimum

requirements within six months of job appointment. Contractor Technical Level I, II and III personnel must also obtain the appropriate computing environment certification/s required by their employing organization. The contractor shall be responsible for yearly maintenance fees to keep these certifications. This includes but is not limited to 120 Continuing Professional Education credits (CPEs) every three years.

Role Requirement:

- Information Technology Service Management (ITSM) - IAT I
- Help Desk Support - IAT I
- Application, Database and Web Administration - IAT II
- System, Virtualization and Mainframe Administration - IAT II
- Network Technicians (non-supervisor) - IAT II
- Network Security Technicians (non-supervisor) - IAT II
- Senior Network Engineer (Supervisor) - IAT III

3.5 Future Projects Migration & Sustainment

3.5.1 It is anticipated that during the life of this contract DMDC will continue to upgrade, virtualize and potentially migrate applications and databases (physically and virtually) to and from other commercial, Government, and/or DoD/DISA owned enterprise computing centers. The Contractor is expected to support migration efforts, sustain and maintain DMDC operated solutions, coordinate efforts with external service providers, implement new in-house solutions, and provide end user support.

3.6 Industry Best Practices

3.6.1 The Contractor will provide best practice solutions and continuous process improvement strategies as part of their solution. Support will be designed to provide highly integrated and responsive technical support that first and foremost, strives to provide an exceptional user experience. The Contractor will accomplish this by providing a structure capable of meeting the needs of DMDCs varied user communities, fostering user confidence and security by providing the highest quality of service to address all registered concerns quickly and accurately, and following through in a manner that considers the needs of the users and the agency.

- Creating and maintaining value for our end users through an enhanced service delivery model that is focused on operational excellence, innovation, and repeatable processes.
- Creative approaches to communicating with users and empowering users to remediate low complexity issues through self-help.
- Resolving incidents and problems and ensuring the delivery of high quality services are delivered as rapidly and effectively as possible.
- Clearly defined and efficient hardware and software asset management.
- Sufficient levels of staff that is technical, knowledgeable of Government processes and adequately trained, certified and monitored.

- Providing expansion capabilities to accommodate increases in user base or advances in technology.
- The contractor will provide innovation, best practices, cost savings/efficiencies, employee productivity, customer service, application availability/performance, and evaluation/recommendation of new technologies to achieve these goals.

3.6.2 Recommend and suggest improvements which optimize performance, eliminate single points of failure, and enhance viability of DMDC Enterprise and/or best postures DMDC for greater capabilities to support the DoD and its customers.

3.6.3 DMDC's rapidly-evolving business and mission environment demands new and improved ways to provide properly secured access through: shared critical business and mission-related information; response to the surging and receding mission needs; unpredictable service and rapidly changing support staffing needs; an ability to leverage existing information assets to meet emerging mission challenges; and optimize the benefits of IT applications expenditures.

3.7 Desired Skills and Knowledge

The contractor must have experience and expertise as an ITSM provider. A management structure is required that can effectively manage a professional and technical work force engaged in a wide range of IT related services. The Contractor shall have organizational structure, procedures, and administrative support functions to effectively and efficiently manage the work performed under this contract. Both technical knowledge and project management skills are required to keep up technology and manage the implementation of technology changes being implemented within the technical infrastructure. The management structure shall provide a single point of contact for interface to the Contracting Officer's Representative (COR), work in a professional manner and maintain an adequate and skilled work force to accomplish PWS requirements. Please see Appendix C.

4.1 REQUIREMENTS

The contractor shall provide support to fulfill the Governments requirements by the tasks identified below:

Task 1: Information Technology Service Management (ITSM)
Task 2: Security Compliance and Path Management
Task 3: Server Administration
Task 4: Network and Telecommunications Management
Task 5: Virtualization Administration
Task 6: Web Middleware Administration
Task 7: Database Administration
Task 8: Provide Help Desk Services
Task 9: End User Devices and Peripherals Administration
Task 10: System Build, Integration and Testing Environment
Task 11: Mainframe Support Services

Task 12: Mainframe Application Programming (Optional Task)
Task 13: Future Projects and IT Services (Optional Task)
Task 14: DMDC Registration Authority (Optional Task)

For each task, the contractor will:

1. Ensure all projects are in compliance with stated and referenced Policy and Directives.
2. Capture meeting minutes and action items at every meeting. The meeting minutes and action items will be sent out within 48 hours after the meeting.
3. Attend their assigned Branch's meetings and communicate project and/or task status as indicated in the PWS.
4. Work with the Government to ensure all projects operate within schedule, performance, and budget baseline thresholds.
5. Have effective oral and written communication skills.
6. The contractor in the last 6 months of the period performance will transfer knowledge on the activities that they perform to Government staff as stated in the transition portion of the PWS.
7. Additionally, the Government encourages the Contractor to propose strategies to improve DMDC processes, policies and procedures within the scope of the anticipated task order to their assigned Contracting Officer Representative (COR). If the COR chooses to implement any proposed strategies, the Contractor will be notified to proceed with an implementation plan that identifies the assumptions, approach, schedule, cost-benefit, dependencies, risks and constraints. Any strategy changes that fall outside of the scope of the task order and affect cost must be vetted through the COR and approved prior to submission by the CO.

4.2 TASK 1 – Provide Information Technology Service Management (ITSM)

4.1.1 Project Management

The DMDC Project Management lifecycle is consistent with the Systems Development Lifecycle (SDLC) and cover all necessary aspects of Project Planning, Initiation, Execution, Monitoring and Control, and Closeout to effectively manage and control project performance and progress towards stated objectives. These services include identifying project scope, defining schedules and actionable task items, tracking of progress and milestones, reporting of project status, and completing projects on-time with allocated resources.

a. Capability Requirements – The contractor shall:

4.1.1.1 Be responsible for the day-to-day management of the project and delivering the means, methods, and resources to ensure the requirements are value added and necessary to achieve project success. Manage projects associated with the modernization and expansion of the technology infrastructure that supports DMDC's mission. The scale of projects managed includes small single site projects to large enterprise projects with independent project lifecycle durations of several months to multiple years. During the course of managing project lifecycles, the Contractor interfaces with stakeholders throughout DMDC, other federal agencies and commercial vendors on

a daily basis. The project management lifecycle shall be consistent with the Systems Development Lifecycle (SDLC) and cover all necessary aspects of Project Planning, Initiation, Execution, Monitoring and Control, and Closeout to effectively manage and control project performance and progress towards stated time-lines, milestones, task/s and objectives.

4.1.1.2 Provide strategic and implementation planning, project integration, coordination, technical support and other related IT tasks. Prepare and maintain a detailed project management plan (PMP) for IT projects that identifies and assigns tasks, major milestones for the efforts of the project team, the estimated dates on which they occur, dependencies, indications of critical path and potential risks and gaps.

b. Subtasks:

4.1.1.3 Document all support requirements in a Project Management Plan (PMP). The PMP shall describe the proposed management approach and include milestones, tasks, and subtasks required in this contract. The PMP shall provide for an overall Work Breakdown Structure (WBS) and associated responsibilities. The PMP shall include the contractor's Quality Control Plan (QCP) and is an evolutionary document. It shall be updated quarterly and approved by the Government.

4.1.1.4 PMP will include the status, statistics; risk management review; critical path and other milestone progress checks and updates; as well as technical content review. Develop and implement PMP's that identify the management strategies to be followed and goals to be achieved. Project Plan must be current within five business days at any time during the project. The project plan must take into consideration the availability of available resources to complete each project while those resources are supporting other projects and operations. Tasks will be selected as milestones against which progress will be monitored. The project plan is a formal, Government approved document used to manage project execution and control and shall encompass all the tasks for IT Operations projects. The plan, at a minimum should contain:

- Name of the Project Manager
- Roster of required team members and functional expertise
- The project's strategy (lifecycle, scope, major activities, reviews, test) and delivered product
- A manageable breakdown of the total work that will be done during the project provided as a WBS with monthly progressions
- Identify milestones, description and dates
- Key risks, including constraints and assumptions and planned responses for each
- Bi-weekly status reports reflecting accomplishments and any issues related to the project
- Scope management
- Requirements management
- Technical management, including applicable standards
- Configuration/change management (CM)
- Schedule management, including detailed schedule in MS Project

- Resource support
- Communications management
- Risk management
- Quality management
- Dependencies
- Indications of critical path
- Critical production issues
- Planned and unplanned outages
- Work Breakdown Structure, including consideration of balancing resources across projects and operational requirements

4.1.1.5 Create a Communication Plan to identify and track all required communications in support of the PMP. The Communication plan will identify all key stakeholders and identify the appropriate communications format (examples include: meetings, briefings, SharePoint) content and schedule for each stakeholder. Submit to COR, IT OPS Director and IT OPS Deputy Director 30 days after contract award.

4.1.1.6 Develop and maintain a decision log to provide a concise, centralized record of all decisions, approvals or agreements affecting the scope, schedule, or internal and/or external deliverables for the project. Project priorities will be set by the Government based on organizational requirements and complexity.

4.1.1.7 Maintain, refine, and revise the project collaboration sites on SharePoint. The DMDC internal site must include project overview documents; a consistently updated document library that preserves document history; schedules; a dashboard; assignment and POC lists; summaries and agenda for all meetings and conferences attended; and support for collaborative editing/versioning of project documents.

4.1.1.8 Improve Project Management Process Maturity Level (pursuant to existing DMDC Capabilities Maturity Model Integration - Information Technology Infrastructure Library (CMMI-ITIL) Assessment Criteria and Assessment Baseline documentation).

4.1.1.9 Quarterly analyze project portfolio to determine the optimal mix and sequencing of interrelated project requirements and activities to achieve the most effective and efficient consolidated use of resources, cost, labor, infrastructure and technology.

4.1.1.10 Determine available meeting locations, teleconference bridges and develop agenda and meeting minutes. Capture action items, resolutions and document decisions identified during meetings and distribute in a time established by the Government. Facilitate, capture and document project lessons learned.

4.1.1.11 Maintain a master calendar of all projects and the major milestones for each to provide a high level executive picture of all project activities. Submit to CO and COR 30 days after contract award. A list of all known projects is provided in Appendices.

4.1.1.12 Meet or exceed the established Acceptable Quality Levels/Key Performance Indicators as identified in Appendix A.

4.1.1.13 Attend a bi-monthly project review meeting to discuss status of all projects and provide updated information regarding the "health" of the high visibility projects. The "health" should include current status, risks, issues, concerns, hurdles, recommendations for improvement and implementation strategy of recommendations.

4.1.2 Information Technology (IT) Service Portfolio Management

DMDC Information Technology (IT) Service Portfolio Management is concerned with delivering and supporting IT services that are appropriate to the business requirements of DMDC. IT service quality is maintained and improved through a constant cycle of agreeing, monitoring and reporting to meet the customer's' business objectives. The 'portfolio' of services represents the services the DMDC IT Operations division delivers and documents future planned IT services. DMDC IT Service Portfolio Management enables the IT Division management to make sound decisions about investment for IT services.

a. Capability Requirements – The contractor shall:

4.1.2.1 Be responsible for research and analysis on best technology practices, ensuring that IT strategy meets overall business strategy. Establish a robust IT Service Portfolio to account for IT services and to attribute these costs to the IT services delivered to the organizations internal and external customers.

b. Subtasks

4.1.2.2 Complete the creation of an IT service catalog (approximately 10% completed) and support the development of a chargeback model to assist the Government in selecting services and management in developing detailed business cases and cost models for calculating the cost of IT services. The catalog will identify the services along with the definition/description, category, dependencies, and service level agreement (SLA).

4.1.2.3 Perform an annual portfolio analysis to identify and recommend applications rationalization, consolidation, lifecycle replacement, etc. Continuously review the portfolio of services for applicability and demand.

4.1.2.4 Facilitate the monthly IT Portfolio Review meeting, including the review of projects entering the execution pipeline, reviewing the forecast of upcoming releases, and leading discussion regarding schedule, conflict, and resolutions. Assist Government in aligning projects with organization priorities and capabilities.

4.1.2.5 Assess the underlying IT environment within the organization making recommendations on how to achieve long-term scalability, reduce operational cost and better support business processes.

4.1.2.6 Conduct feasibility studies for the implementation of new technologies; Identify possible product and software tool enhancement opportunities for improved performance and potential cost savings.

4.1.2.7 Provide a Technical Refresh Plan (TRP) to support programmatic growth to include addressing user expansion and technology refreshment planning for all hardware, software and middleware used. The TRP will include a methodology that determines the best approach and timing for design refreshment, and the optimum mixture of actions to take at those design refreshes as needed.

4.1.3 Asset Management

DMDC Asset Management is a standard accountancy process concerned with the asset lifecycle from procurement, asset receipt, tracking, maintenance, transfer and disposal of assets. Assets include: hardware, software, consumables, maintenance contracts and procurements for the DMDC Enterprise. Asset Management function maintains an asset management database which maintains and tracks information such as asset values, asset disposition, current ownership, End of Support Life (EOSL) and location of assets. The role of the DMDC Asset Management Process is the oversight, support, communication and maintenance of the Asset Management Process Standard DMDC enterprise wide.

a. Capability Requirements – The contractor shall:

4.1.3.1 Maintain inventory of all hardware and software licenses, procurements and maintenance contracts. Make available to the Government electronic reports detailing current assets, and manage an IT Asset Management Program that provides end-to-end asset inventory solution for all IT assets.

4.1.3.1Maintain Deployable Technology List of all software approved for use or removal within enterprise. Additions and removals from the list shall be made within 30 days of approved change.

4.1.3.2 Maintain the DMDC web-accessible information store of IT asset data and software data repository to be referred to as the Configuration Management Database (CMDB) or equivalent. DMDC currently uses the CA Unicenter tool. Integrate the CMDB Tracking System with incident/problem tickets, change order tickets, configuration and knowledge management documents. Inventory catalog should accurately reflect asset data for all IT assets in the DMDC enterprise in the NIPRNET and SIPRNET environments.

b. Subtasks

4.1.3.3 Be responsible for the scheduling and occasional transfer of GFE equipment within the Washington D.C. Metropolitan area (site to site), in compliance with DoD regulations and guidelines regarding GFE equipment, when requested by the Government.

4.1.3.4 Support Defense Reutilization and Marketing Office (DRMO) procedures at DMDC. Identify and prepare EOSL equipment within two weeks of removal from inventory. Prepare IT assets for disposal and shipment by sanitizing and excessing assets in accordance with DRMO policy. Notify the Government POC's (ITO & Human Resources & Facilities) quarterly when excess to DRMO is required.

4.1.3.5 Maintain and keep current the DMDC Asset Management Standard Operation Procedures (SOP) outlining duties and responsibilities. Publish and maintain policies, process, procedures and checklists related to the Asset Management function. Documentation shall be available on the DMDC intranet (SharePoint and/or Service Desk Tool). Provide required reports, inventories, and property control procedures.

4.1.3.6 Maintain a Consumable Inventory reflecting the current inventory status and forecasting future requirements to include the following consumable items: printer toner, printer replacement parts, such as fusers and drums, CAC readers, projector light bulbs, natural keyboards, specialty mice and trackballs, microphones, and webcams. Report should also show the previous three month replacement needs, and recommendations for future purchases of consumable items to ensure a stock is always on hand and readily available to prevent future service outages due to not having available stock.

4.1.3.7 Ensure all IT equipment is properly bar-coded and entered into the inventory management system within 5 business days after receipt. Track any equipment changes.

4.1.3.8 Ensure all IT equipment status changes are properly documented in the inventory management system within 1 day of the change.

4.1.3.9 Perform an annual inventory of all physical IT assets, updating the CMDB (or equivalent). Initial inventory will be performed within 90 days of contact award. Provide a report 30 days after the completion of the inventory, regarding the accuracy of the inventory, types of issues encountered, corrective actions and dates in which the corrective actions are to be completed to ensure ongoing maintenance of the CMDB.

4.1.3.10 Perform review as requested by the Government of software license counts ensuring non-overuse of utilized software. Maintain continuous maintenance contract status via the current Dashboard or equivalent. Make available on the dashboard a report for software license count usage issues and maintenance support contract disposition to ensure contract continuity.

4.1.3.11 Provide an Asset Management Point-of-Contact at each operating site, to facilitate Asset Management duties within 90 days after contract award.

4.1.3.12 Ensure maintenance coverage on IT Assets, (hardware and software) advising Government within six (6) months minimally ahead of equipment nearing End of Lifecycle.

4.1.3.13 Notify the Government not less than 12 months prior to the date on which software/hardware becomes unsupported or decommissioned by the manufacturer. In the event that a vendor announces the withdrawal of support or decommission of a product less than 12 months in advance, then notify the Government as soon as possible, but no later than 15 calendar days from the date of the announcement.

4.1.4 Event, Incident & Problem Management

DMDC Event and Incident Management goal is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations. Problem Management goal is to minimize the adverse impact of Incidents and Problems on the business that is caused by errors within the IT Infrastructure, and to prevent recurrence of Incidents related to these errors. At DMDC, this is accomplished with DMDC partnership with the Consolidated Contact Center (CCC)/DMDC Support Center (DSC). The CCC/DSC has the responsibility for fielding calls from external end users and providing the central meet-me-line for incident coordination.

a. Capability Requirements – The contractor shall:

4.1.4.1 Monitor and respond to production system events and incidents. Respond on a 24x7x365 basis to incidents impacting service availability.

4.1.4.2 Support Incident Management processes in responding to all service outages; system administration, network, telecommunications, virtual administration, web middleware administration, database administration, SAN administration, Cluster Management, etc. Availability is required via on-call support on a 24x7x365 basis at the declaration of an incident and must be engaged through service restoration.

4.1.4.3 Partner with the capacity management team for any trends, ensuring space and capacity do not become an incident. Coordinate with the application stakeholders to determine the proper event threshold levels.

4.1.4.4 Manage, identify/classify, record, correlate, categorize Problem Management Incident Report (PMIR)/Major Problem Review (MPR) and Internal Problem Review (IPR) activities and provide after action review boards with those outages that are deemed necessary by Government. After PMIR/MPR and IPR activities develop, assign and track corrective and preventative action items until resolution. Team will work across divisional lines, internal/external to ensure production outages are resolved timely and not repeated if within IT Operations Division responsibility.

4.1.4.5 Restore normal operation after incident, prepare root cause analysis, applying ITIL Best Practices ensuring business impact is minimized and no further production outages occur.

b. Subtasks

4.1.4.6 Schedule all planned downtime as to minimize impact to users and communicate planned events and expected restoration time to affected users no less than 2 business days before the event.

4.1.4.7 Respond to Production outages within 10 minutes of initial contact from CCC/DSC to the Incident Manager.

4.1.4.8 Coordinate with IT Operations teams and/or cross divisional groups to isolate/identify/resolve Incident.

4.1.4.9 Provide stakeholders with hourly updates in the event of an unplanned end user computing outage or a planned outage which lasts longer than originally scheduled.

4.1.4.10 Upon receipt of system failure/incident notification, treat the incident as priority level 1until identified otherwise. Priority levels are defined in the SOP's. Provide Incident Manager(s) for each service outage to coordinate and triage trouble shooting efforts through successful service restoration.

4.1.4.11 Revise the current Event Management Program to include updated thresholds, logical notifications and revised documentation using Best Practices to ensure a robust Event Management Monitoring System. Use current Tool or recommended solution.

4.1.4.12 Categorize and correlate events to trigger the correct response or escalation to incident management.

4.1.4.13 Establish and maintain a fully functional Incident and Problem Management Program, in accordance with DMDC SOP see Appendices.

4.1.4.14 Document the lifecycle of an incident (production outage) from start to finish utilizing: checklists, SOPS, and lessons learned for each production environment.

4.1.4.15 Log, categorize and conduct an initial diagnosis of incidents. Provide a near-real time status of all IT incidents coordinate with problem management on cause, resolution and prevention of incidents.

4.1.4.16 Apply known errors and established workarounds during Incident Management/Production Outages to restore service. Document errors and workarounds when

identified during Incident Management/Problem Management and make available in a knowledge base (i.e. SharePoint and/or Service Desk Tool).

4.1.4.17 Contact support vendor to open a support ticket with the vendor, creating the appropriate DMDC Internal Incident ticket with the vendor ticket contained. Ensure email notification developed and forwarded to designated DMDC staff and management. The Contractor shall support vendor updates will be provided every thirty minutes ensuring visibility of latest details.

4.1.4.18 Provide PMIR/MPR and IPR report within five days (Government may request the report soon depending on the severity of the outage). The information in the report should be based on similar outages, discussions with subject matter experts and review of documentation. Include in the report, narrative of the outage, meeting discussion notes, action items/assignments, recommendations and preventative actions. Prepare trend analysis, target preventative actions and track actions until resolved.

4.1.5 Capacity Management

DMDC Capacity Management is responsible to ensure that cost-justifiable IT capacity for all areas of IT always exists and is matched to the current and future needs of the business. Capacity Management is a process that extends across the service lifecycle and it is considered during the service design stage. DMDC Capacity Management considers all resources required to deliver the IT service, and plans for short, medium and long term DMDC business requirements. The Capacity Management works closely with the other DMDC ITIL functions to ensure exhausted capacity does not result in an incident.

a. Capability Requirements – The contractor shall:

4.1.5.1 Maintain a fully functional Capacity Management Program to include the following activities: Capacity Planning and Analysis, Measured performance results, Performance Management and Analysis and Reports, Proactive Modeling and Forecasting, New Application and Major Upgrade Sizing Formalized Measurement, Auditing and Compliance Capacity forecasts.

4.1.5.2 Ensure all current and future capacity and performance aspects of the business requirement are provided by using ITIL Best Practices, standardized methods and processes.

4.1.5.3 Measure Process Compliance (Key Performance Indicators (KPIs), Monthly/Quarterly Reporting/CMMI-ITIL Maturity Assessment) and escalate exceptions to the Government (See Appendices – AQL/KPI).

4.1.5.4 Produce and maintain the specific subject matter for reporting and capacity plan development (processor, memory, space allocation, storage requirements, proposals for configuration changes, etc.).

4.1.5.5 Perform capacity workload planning, reporting and availability analysis for a variety of applications and components, and develop and execute capacity projection plans. Ensure resource requirements are met, reported on, and communicated to product owners and management teams.

b. Subtasks

4.1.5.6 Allocate storage space, plan for future projects or acquisitions, review hardware and software configurations and make suggestions for appropriate storage or backup models.

4.1.5.7 Maintain storage devices, analysis of capacity, and provide monthly capacity reports for the storage device, system, or component.

4.1.5.8 Maintain servers, server appliances, storage area network (SAN), fabric , routers, network switches, firewalls, load balancers, storage devices, analysis of capacity, and provide monthly capacity reports for those devices, systems or components.

4.1.5.9 Provide Data Center and Infrastructure Capacity Management processes that avoid capacity-related service disruptions; alert the Government when established performance threshold are exceeded; determine underutilized resources that may be candidates for consolidation or elimination.

4.1.5.10 Monitor daily performance and quality of service and report on efficiency and effectiveness of the Capacity Management process. Capacity Management shall protect services from capacity related incidents and service downtime and minimize capacity related incidents/problems by proactively monitoring. Notify the Government of any anticipated incidents/problems to determine resolution.

4.1.5.11 Provide a Monthly Capacity Report that provides service management processes and shows metrics to demonstrate system performance health. Maintain a performance reports database.

4.1.5.12 Gather historical performance data and business driver data and assesses whether systems are performing according to production standards, thresholds set by the Capacity Planning team.

4.1.5.13 Generate and present enterprise capacity planning reports; engineer, support and maintain capacity and performance planning tools.

4.1.5.14 Establish proactive analysis and root cause analysis capabilities for use by any technology teams in DMDC.

4.1.6 Availability Management

DMDC Availability Management optimizes the capacity of the IT Infrastructure, services and supporting organization to deliver a cost effective and sustained level of availability that enables

DMDC ITO to satisfy its business objectives. DMDC Availability Management covers the design, implementation, measurement and management of IT infrastructure availability.

a. Capability Requirements – The contractor shall:

4.1.6.1 Produce and maintain an appropriate and up-to-date Availability Plan that reflects the current and future needs of the business.

4.1.6.2 Monitor, report, analyze and review service availability. Assess and manage risk by implementing preemptive and corrective countermeasures to ensure availability.

b. Subtasks

4.1.6.3 Establish a robust comprehensive reactive and proactive ITIL based Availability Program to ensure DMDC IT services are in good health and available for customer access. Provide solid availability, reliability, maintainability and resilience within the enterprise.

4.1.6.4 Establish and implement a documented outage management process that is used to plan, schedule, execute, monitor, and document outage activities.

4.1.6.5 Communicate planned outages in a manner that will allow customers to understand the impact to their area. Ensure outages have been properly coordinated and approved by customers prior to implementation. Multiple notices shall be sent as outage period approaches.

4.1.6.6 Perform outages and execute maintenance actions during non-mission critical and off-shift timeframes in order to minimize risk to program operations and to limit impacts.

4.1.6.7 Maintain and update the database of assigned systems, their input requirements, and their impacts of service disruptions for use in the service restoration process.

4.1.6.8 Maintain and publish (on the DMDC intranet) a daily outage schedule for assigned systems. Update at least daily with any changes or additions.

4.1.7 Change and Release Management

DMDC Change Management is the IT Service Management (ITSM) process responsible for all changes. The purpose of Change Management is to control the lifecycle of all changes - ensuring that all changes to configuration items (CIs) are recorded. DMDC Change and Release Management ensures standardized methods and procedures are used for efficient and prompt handling of all changes to minimize the impact of change related incidents and improve day to day operations. Release Management takes a holistic view of a change to an IT service and should ensure that all aspects of a Release, both technical and non-technical are considered together thereby reducing potential production outages.

a. Capability Requirement – The contractor shall:

4.1.7.1 Maintain and improve the Change and Release Management Program to include the following activities: Governance Framework, Change Control Process Phases, Raising and Recording, Assessing and Authorizing, Planning and Implementation, Post Implementation Review, Closure and Formalized Measurement, Auditing and Compliance.

4.1.7.2 Team with other members of the DMDC Service Management community to provide standardized end-to-end support and act as primary focal point for all changes within the DMDC infrastructure, while providing ongoing development and maturation of the Change Control processes.

4.1.7.3 Demonstrate measurable improvement of Critical to Quality (CTQ) and Critical Success Factor (CSF) Milestones during quarterly review cycles, as measured by positive quarterly trends in the efficiency and CMMI-ITIL Process Maturity rates for Change Management.

4.1.7.4 Perform release and deployment management functions.

4.1.7.5 All Scheduled outages will be approved by the Government (i.e. VOIP, Infrastructure).

b. Subtasks:

4.1.7.6 Use standardized methods and procedures are used for efficient and prompt handling of all changes in order to minimize the impact of Change-related Incidents upon service quality, and consequently to improve the day-to-day operation.

4.1.7.7 Ensure that changes are recorded and then evaluated, authorized, prioritized, planned, tested, implemented, documented in Configuration Management Data Base (CMDB), and reviewed in a controlled manner.

4.1.7.8 Ensure that Critical Success Factors (CSF) and Critical to Quality (CTQ) dependencies are addressed and provided within the DMDC Change Management (CM) System. Examples to include are:

- Appropriate Classification (Routine, Standard, Emergency, etc.)
- Categorization (USD category areas and organizational attributes) of all changes
- Successful implementation of changes
- On-time implementation of changes

4.1.7.9 The Contractor shall: establish, identify, apply and implement the following ITIL Best Practices focusing on the items below within the Change Management Team:

- Mandatory Checklists for Commissioning / Decommissioning evolutions.
- Proper Configuration Item (CI) attachments on all Change Requests that involve changes to any existing CI.
- Proper parent/child attachments and proper Incident/Problem ticket reference correlation.
- Integration of Change Management Process and Short-Term Planning meeting in order to streamline scheduling conflicts and ensure adequate post change test & acceptance. Provide planning calendar to identify potential scheduling conflicts with outage and resources. The calendar should consider scheduled outages identified from change and release management, short term planning and other groups. The planning calendar should be made available via DMDC's intranet or application.
- Implementation and organizational Adoption of standard CR templates (already developed) for common, cyclical or minor CR's to streamline the formalized process and ensure due diligence is given primarily to the 20% of Changes which have 80% of the Production Impact potential.
- Mechanism to implement High Priority (Urgent/Critical/Emergency) Changes without compromising quality assurance and system performance. Mechanism to capture Root Cause of High Priority Changes (unplanned and otherwise) and drive down the rate of high priority (emergency/critical/urgent) changes.
- Workflow and checkpoint improvements to ensure Change Advisory Board and Technical Review Board/Change Control Board (TRB/CCB) functions do not become a "rubber stamp" and actually add quality control value to the Change Control process.

4.1.7.10 Report Operational Change Management Metrics in accordance with CMMI-ITIL Process maturity rates for Change management and KPI criteria. Reviews will require no more than two quarterly review cycles to meet acceptance levels. Key Performance Indicators should reflect positive monthly and quarterly trends in the accuracy and quality of existing Change Requests (CRs).

4.1.7.11 Prepare, build, and test deployment packages and conduct pilots as necessary to ensure successful change implementation.

4.1.7.12 Develop, maintain, and publish on the DMDC intranet, a release calendar of all scheduled changes and application deployments. To be updated on the 1st of every month.

4.1.7.13 Coordinate and facilitate release planning meetings with stakeholders and implementation teams. Identify and resolve scheduling conflicts and dependencies and confirm the release calendar.

4.1.7.14 Manage the deployments of changes and applications.

4.1.7.15 Verify and monitor early life of fielding and correct any issues. All deployments should have a minimal impact on the customer and operations.

4.1.7.16 Ensure back out plans exist and execute when necessary due to adverse or unanticipated impact of changes or deployments.

4.1.7.17 Review existing change management and track policy and procedures and update them as needed to address change requests and application defects from receipt through review, analysis, development, and installation.

4.1.8 Configuration Management (CM)

Configuration Management (CM) refers to the discipline of evaluating, coordinating, reviewing, and implementing changes in artifacts that are used to construct and maintain software systems. Software Configuration Management (SCM) is the task of tracking and controlling changes in software as well as reporting current status and change history of software components (including source code, documentation, problems, changes requested, and changes made). The goal of SCM is to establish and maintain the integrity of software components from initial concept through design, implementation, testing, base lining, building, release, and maintenance by ensuring configurations are properly evaluated, authorized, and implemented.

a. Capability Requirements – The contractor shall:

4.1.8.1 Maintain, update and improve existing Configuration Management program that addresses all new and/or modified hardware, firmware, software and documentation. The program shall define the Configuration Items (CIs), establish and document the Configuration Management processes, improve on the current configuration control and change management process, establish release cycle baselines/documentation, establish a verification process, and other areas of Configuration Management Governance. Automated tools will be used for a positive Return on Investment (ROI). This Configuration Management program shall be planned, documented and established with direct coordination and phase approval of the Government.

4.1.8.2 Perform CM activities of configuration status accounting, configuration baseline management, creating and maintaining a Configuration Management library system to control the release of products and manage their history, and administering a centralized change management procedure and centralized tool to track all change requests (CRs) or problem reports (PRs) to the baseline as well as all issues (problem reports). This includes Commercial Off the Shelf (COTS) and Government Off the Shelf (GOTS) software, database deployable objects, and hardware. The

Contractor shall respond to documents delivered with the software release. Update and re-deliver documents if not approved.

4.1.8.3 Design, publish, and implement transition plan from homegrown CM Tools to modern scalable industry standard tools including a unified change management system for hardware and software changes (including COTS) that has approval workflow and task routing and graphical user interface to the automated build and deployment scripts (shell scripts, python, and WLST)

4.1.8.4 Identify, describe, and track software and hardware configuration items and their dependencies

b. Subtasks: The Contractor shall:

4.1.8.5 Record, track, and report on all deviations from CM standards

4.1.8.6 Review and grade completed production level changes for accuracy, completeness, adherence to process & standards

4.1.8.7 Perform random auditing to compare CMDB to actual deployed version on servers

4.1.8.8 Monitor, fine tune, and update the build/deploy automation scripts to incorporate changes in policy or environment

4.1.8.9 Oversee build & deploy automation work, proactively review issues and failures, fix them, resubmit failed attempts, and document issues and fixes

4.1.8.10 Perform release management functions for DMDC - coordinate software releases among all divisions

4.1.8.11 Design, implement, and maintain release strategies for the DMDC Common Update Framework

4.1.8.12 Publish and make available dynamic real-time reports for all (daily, weekly, monthly, and biannual) DMDC production releases to include item name, item version, QA status, current environments deployed to, release date, dependencies

4.1.8.13 Software Request for Change Approval Process (SharePoint workflow & InfoPath Forms) - manage the "Request for Change" workflow which runs on SharePoint using InfoPath forms

4.1.8.14 Source Control software management & account provisioning (Collabnet Subversion Edge) - manage and maintain the source code repository and repository admin tool

4.1.8.15 Technical Review Board for software changes - Technically evaluate proposed changes for feasibility, timeline, risk, etc. & ensure documented requirements are met for production deployment

4.1.8.16 Manage DMDC's implementation of Maven. Manage and maintain DMDC's Maven Repository and Maven Sites reports

4.1.8.17 Manage and Maintain DMDC's Java Deployable Technology List (java DTL)

4.1.8.18 Manage the CM Work Queue (currently CA UniCenter Service Desk.) Assign all tickets to individuals in the time specified by DMDC policy

4.1.8.19 Triage failed builds and deployments. Review build/deployment script logs and server logs to help recognize patterns of failure. Categorize and track failures and work with other teams to identify root causes and implement fixes

4.1.8.20 Perform manual deployments to application servers if automation is not working properly

4.1.8.21 Maintain software Web Application CMDB which supports automated and manual software web application deployments and application release governance.

4.1.8.22 Provide technical support and assistance that corrects all systems malfunctions, maintenance of new and modified systems and applications software to assure availability, operability and efficiency.

4.1.8.23 Maintain Web Application CMDB software that supports automated and manual application deployments and release governance.

4.1.8.24 Provide technical support for the existing build and deployment automation scripts to include full-time subject matter expertise in Python, Perl, WLST (WebLogic scripting tool), and traditional UNIX shell scripting.

4.1.8.25 Analyze the needs and capabilities of the automated build and deployment system, research industry standards, provide recommendations for possible replacement by COTS solutions, install, manage and perform the day-to-day functions, including troubleshooting, requirements updates, and general maintenance of the new solution or existing scripts.

4.1.8.26 Provide a CM Plan that follows industry standards and applies to the hardware, software and documentation developed, maintained, or operated by the enterprise.

4.1.8.27 Provide all baseline system documentation that includes system designs, build procedures, requirements documents test procedures, problem reports, software code, and system knowledge base and deliver to the Government upon final Government acceptance. Ensure IT configuration

changes are documented in CMDB. Ensure changes are approved and executed is in accordance with DMDC governance practices.

4.1.8.28 Document CI dependencies in the CMDB between hardware, software and other IT assets. Update relevant CMDB CI relationships as configuration changes are executed.

4.1.8.29 Include in the Monthly Change Report submitted on the **4th of the month**, the date the change ticket was opened, users affected, nature of any changes and the status of the implementation of the change.

4.1.8.30 Evaluate proposed Configuration Management changes and provide solutions to improve the quality of the change package and/or its likelihood of successful deployment.

4.1.8.31 Update the deployment calendar quarterly for routine infrastructure software, network and database upgrades (O/S, browsers, databases, web applications, etc.) on SharePoint.

4.1.8.32 Provide a quarterly status of infrastructure upgrades (completed, on time, behind schedule, delayed, postponed, etc.).

4.1.8.33 Provide maintenance support for CMS GOTS application utilizing Microsoft Access database and Oracle database for policy or ownership changes.

4.1.9 Knowledge Management (KM)

The IT Operations Division currently maintains over 300 Knowledge Articles, including how to documents, in the Knowledge repository with an additional 300 documents, including policies, forms, processes and procedures, are also managed on the internal SharePoint portal.

a. Capability Requirements – The contractor shall:

4.1.9.1 Provide Knowledge Management support services that streamline and improve KM processes. Facilitate, train and sustain the ability of KM users to interface with IT Operations

4.1.9.2 Facilitate the creation and advancement of KM process improvement initiatives such as self-help.

4.1.9.3 Provide documentation and technical writing services that are typical to IT projects and in support of ITSS initiatives.

b. Subtask:

4.1.9.4 Provide documentation and technical writing services that include developing and maintaining documentation related to hardware, software, PKI, division processes and policies and resources/tools.

4.1.9.5 Develop new and review and update, when necessary, existing training materials, forms, templates, checklists, how-to documents, and SOPs. The stakeholders are both Division customers needing access to services or self-help tools as well as internal system administrators and technicians who standardize repeatable processes.

4.1.9.6 Develop and post DMDC wide announcements (i.e. SharePoint, Service Desk). All announcements must be approved by a Government POC before being posted.

4.1.9.7 Improve KM integration with the current or a replacement Service Desk Tool with SharePoint ensuring maximum user access to a self-service knowledge management environment based upon authentication and authorized use.

4.1.9.8 Restrict access to knowledge for different user communities.

4.1.9.9 Technical Writing

4.1.9.9.1 Provide technical writing tasks include; developing and maintaining documentation related to the ITIL processes, and/or on-line (web site) sources of data, developing training materials and documentation, developing Standard Operating Procedures (SOP's) and documenting key meetings.

- Maintain the IT Operations documentation library
- Develop and maintain user documentation and on-line help
- Develop training materials and documentation
- Develop documentation of systems, and processes
- Document meeting minutes for key meeting
- Develop and maintain Standard Operating Procedures (SOP's)

4.1.10 Disaster Recovery (DR) and Continuity of Operations (COOP)

a. Capability Requirements – The contractor shall:

4.1.10.1 Perform analysis of the DMDC services and maintain, update, or develop plans, processes, procedures, and training materials for restoration of operations in the event of an incident or disaster.

4.1.10.2 Conduct ongoing gap analysis across the DR Program to ensure identification of gaps in planning, documentation, implementation, testing, training, and exercises. Take corrective action to remediate any gaps or issues.

4.1.10.3 Provide management of accounts, network rights, and access to systems and equipment; maintain the integrity of system baselines and provide audit checks of all systems and backups as required; identifies and documents the functional and physical characteristics of the system CIs), controlling any changes to such characteristics, records and report the change(s) within the

Configuration Management Database (CMDB) with the implementation status and validates conformance to requirements.

b. Subtasks:

4.1.10.4 Maintain, update, and test the Disaster Recovery Plan for restoration of operations in the event of an incident or disaster on NIPRNET and SIPRNET. Conduct ongoing gap analysis across the DR Program to ensure identification of gaps in planning, documentation, implementation, testing, training, and exercises. Plan should meet the requirements in NIST 800-84. Provide Disaster Recovery Plan 60 days after contract award.

4.1.10.5 Develop system and network designs that enable business and network operations capable of surviving individual component failure.

4.1.10.6 Provide input to the Government for making system degradation decisions in the event of a disaster or incident and lessons learned following exercises.

4.1.10.7 Execute the service failover COOP requirements and DR plan in the instance of a disaster or emergency.

4.1.10.8 Develop and provide an annual update to support, plan, and execute switchover exercises of the Disaster Recovery Plan (DRP). This exercise will be performed at least annually and consists of a full switchover of production IT services from the primary facility to the alternate facility and back.

4.1.10.9 Identify, define, or develop as necessary, guidelines for off-site storage, replication, physical security, scrubbing of hardware (cradle to grave), as they relate to all elements of DMDC security.

4.1.10.10 Develop the long-term strategy based upon the results and prioritizations of the DMDC Mission and Strategic Plan, and the needs of the agency. Assist with development and annual review of Contingency Plan Test Plans to ensure DR requirements are completed and documented, ensuring consistent application throughout the DMDC enterprise.

4.1.10.11 Identify and minimize reliance on resources or entities outside DMDC control and test DR fail-over capabilities as directed by the Government. Develop contingency test plans, lead tabletop exercises and assist with gathering IT related follow up actions.

4.1.10.12 Exercise the COOP failover annually with an option to request a semi-annual test, including a full switchover of production IT services from the primary facility to the backup facility and back. Document outcome of COOP failover test with lessons learned and provide to Government within 30 days of the exercise.

4.1.10.13 Provide back-up and COOP capability for specified data bases, optimizes system efficiencies, generate performance reports, and ensure data is only accessed by authorized personnel.

4.1.10.14 Participate in the evaluation of new products and develop requirements documents and criteria spreadsheets.

4.1.10.15 Maintain COOP documentation and complete COOP testing as scheduled in the project plan.

4.2 TASK 2 – Security Compliance & Patch Management

Cybersecurity is directed by the DMDC Cybersecurity Branch. Security compliance and patch management is a crucial element in systems administration and IT operations. IT security planning, implementation, and compliance is integral to all work performed at DMDC and, therefore, participation is a shared responsibility. The contractor is responsible for continuing to maintain security compliance support and performing patching. Patch Management is one of the major features of the enterprise suite. It encompasses researching, testing and deploying patches for remediation of vulnerabilities identified by security tools managed by the Cybersecurity Branch.

a. Capability Requirements – The contractor shall:

4.2.1 Perform Information Assurance Vulnerability Management (IAVM) compliance patching on all servers, workstations and all other IAVM applicable assets on both the SIPRNET and NIPRNET networks. Remediation is to be completed according to IAVM guidelines. Report IAVM patch compliance to the Cybersecurity Branch according to reporting guidelines.

4.2.2 Implement, maintain and comply with USCYBERCOM Orders and Directives. Implementation is to be completed according to USCYBERCOM guidelines and approved by the Cybersecurity Branch. Report compliance to Cybersecurity Branch.

4.2.3 All DMDC IT assets must meet Security Technical Implementation Guides (STIGs) compliance prior to operating on the DMDC network. Implement, apply and maintain STIG configuration to all IT assets. Deviations from STIG configuration setting must follow the DMDC STIG Deviation process and be approved by the Cybersecurity Branch.

4.2.4 Apply vendor supported security patches on a continuous and timely basis per DoD and DMDC policy. Support third-party software updates and apply definitions to all applicable DMDC IT assets (e.g., network, servers and workstations).

4.2.5 All new IT assets built under this contract and baseline images must go through the DMDC Pre-production process and approved by Cybersecurity prior to operation in a production environment.

b. Subtasks:

4.2.6 Install, configure, and test patches and changes required by Information Assurance Vulnerability Management (IAVM) issuances, vendor patches and STIG configuration items. Implement all necessary changes to Enterprise software and equipment in accordance with the suspense date articulated by the Cybersecurity Branch.

4.2.7 Remediate software vulnerabilities and system misconfigurations identified in the DMDC vulnerability management tool managed by Cybersecurity Branch

4.2.8 Provide a Plan of Actions and Milestones (POAM) for remediation actions that cannot be accomplished by the Cybersecurity Branch assigned completion date.

4.2.9 Provide a STIG Deviation/Non-Compliance report for system configuration items that cannot be accomplished by the Cybersecurity Branch assigned completion date.

4.2.10 Develop and implement a patch management plan that will test and remediate vulnerabilities within the DoD timeline. ~~(currently TASKORD 13-067).~~ Vulnerabilities are completed for critical findings within 7 days of discovery, high within 21 days of discovery, medium within 30 days and lows within 90 days of discovery.

4.2.11 STIG configuration items are to be corrected upon identification by the Cybersecurity Branch.

4.2.12 Gather and collect data to support reporting of IAVM and (Federal Information Security Management Act) FISMA compliance reports and Access and Authorization (A&A).

4.2.13 Exceptions and security non-compliance activity must be processed through and approved by the Cybersecurity Branch.

4.2.14 Document procedures for upgrading and deploying new hardware, software or software upgrades. Test and implement process for upgrades. All DMDC IT assets must be at a compliant and supported version of software and firmware.

4.2.15 Ensure all DMDC IT assets have the required cybersecurity monitoring tools (e.g., tripwire agent, HBSS agent) installed and operational in accordance with DoD and DMDC policy.

4.2.16 All software or hardware patches, updates, firmware must come from the DoD patch repository. Exceptions must be approved by the Cybersecurity Branch prior to engagement.

4.2.17 Provide applications services that are in compliance with and support DoD Public Key Infrastructure (PKI) or IC PKI policies.

4.2.18 Provide solutions that meet confidentiality, data integrity, authentication, and non-repudiation requirements. Solutions shall comply with National Institute for Standards and

Technologies (NIST), Federal Information Processing Standards (FIPS) standards, and DoD or IC standards.

4.2.19 Coordinate patches or changes that require system or application down time with the Government and schedule during allotted maintenance hours.

4.2.20A All workstation and server patches should be completely deployed to all assets, to include laptops, desktop workstations, servers, tablets, etc. Patches should be thoroughly tested for a period of one week on Government approved test machines. Patches should be deployed no later than 14 days after the patch is released, or by the stated deadline presented by DISA/IAVA release management. Report to DMDC designated Government personnel as status of their efforts as requested by management.

4.3 TASK 3 – Perform Server Administration (SA)

The Contractor shall: Upkeep systems configurations and perform operations using privileged accounts on multi-user computer systems (servers). The DMDC system administration staff seeks to ensure that the up time performance, resources, and security of the servers they manage meet the established Service Level Agreements (SLA's) of DMDC. The system administration staff installs, upgrades, patches, remediate computer components and software; provide routine automation; maintain security policies; troubleshoot; train and/or supervise staff; or offer technical support for projects.

a. Capability Requirements – The contractor shall:

4.3.1 Perform administration and maintenance of x86 and SPARC based computer systems running Windows, Linux or Solaris Operating Systems on both the NIPRNET and SIPRNET.

4.3.2 Provide a wide range of system administration services which may include, installing, supporting, and maintaining servers or other computer systems, and planning for and responding to service outages and other problems.

4.3.3 Perform system/application diagnostics through the use of tools to ensure availability and to provide notification of problems to the Government.

4.3.4 Maintain the integrity of system baselines and provide health checks of all systems and backups.

4.3.5 Implement COTS applications as applicable and approved by the Government or develop scripts. Examples of scripting tasks include the automation of the account-creation process, renaming of a wide range of accounts to another naming convention, and automatic notification to users on account statuses based on "triggers." Specifics on what may be required are subject to changes in Government guidance, Agency directives, upgrades, migrations, etc.

4.3.5A Any new software to be used within the DMDC environment will require that an automated software installation package be created for deployment using DMDC's approved automation tool. Upon approval for use, a software deployment package will be created and fully tested. Software packages should be fully tested and available for use within 30 days of receipt.

4.3.6 Provide technical support (Tier II) and assistance that corrects all systems malfunctions, maintenance of new and modified systems and applications software to assure operability, efficiency and compliance with DoD standards.

4.3.7 Provide direct support to customers through rapid response to problem reports/trouble tickets and respond to requested workload through change requests utilizing Information Technology Infrastructure Library (ITIL) principles.

4.3.8 Monitor system and process status on a broad range of UNIX, Linux, storage, SAN switches, blade centers, and Wintel servers on a 24x7 basis. Take the necessary actions to address problems using the Incident Management process, which includes problem identification, resolution, documentation, and transfer of control between teams, vendors, and other personnel.

4.3.9 Perform touch labor on all server/equipment. This would include such items as tape/disc loading, power up/down (as requested by the customer), maintenance vendor escort, validation of interface connections and status light conditions, minor cabling, and occasional operations that can only be performed at the physical system.

4.3.10 Provide expertise support to administer DMDC's SharePoint infrastructure, to include development, management, and support for SharePoint sites, infrastructure and portals. DMDC uses Microsoft SharePoint as their primary documentation repository and is investigating SharePoint cloud services via DISA's cloud computing service

b. Subtasks:

4.3.11 Diagnose software and hardware failures to resolution. Maintain availability of more than 99.5 percent.

4.3.12 Assist the Cybersecurity Branch in the prevention of computer hacking and other security problems by implementing preventive measures in compliance with enterprise architecture. Ensure all intrusion detection or other information assurance/cybersecurity systems are fully functioning with operating systems and are current revisions.

4.3.13 Monitor the performance of the servers/systems and resolve any issues related to the efficient and effective use of them.

4.3.14 Install, support, and maintain a stable, redundant, efficient, and productive computer system and computing environment. These activities include: system software maintenance and updates, ensuring compliance with IT security requirements, user account management,

Configuration Management , system upgrade / improvement, computing operations, maintenance of systems documentation and procedures, and contingency planning.

4.3.15 Maintain daily, weekly, and monthly scheduled network backups; test, restore data as required to support systems and data recovery due to hardware, software, or user error; verify and validate the integrity of the backups; and perform recovery test or drills quarterly. Maintain log identifying media, date of backup, data contained within backup and the location of the media. Test backups at least quarterly to verify the most recent backup can be properly restored.

4.3.16 Current backups are conducted on a daily basis (incremental), with full backups performed on weekends. All other information assurance appliances, systems, network and their appropriate IOS/OS's will be backed up to ensure proper and expedient service restoral in the event of a system outage. Provide a weekly report to IT OPS Management that indicates the status of all backups. Service Level for backups and data restoration is 99%.

4.3.17 Identify and document the functional and physical characteristics of the system (CIs), control any changes to such characteristics, record and report the change(s) within the Configuration Management Database (CMDB) with the implementation status, and validate conformance to requirements.

4.3.18 Monitor and report on the overall health of the supported servers and applications. Provide solutions for application and database issues including capacity, redundancy, replication and performance tuning.

4.3.19 Scripting Management - Ensure that repetitive processes are automated to ensure efficiencies and effective handling of tasks.

4.3.20 Define develops, manage and administer processes used to issue and secure user ID's, passwords and security keys (public/private, unique) in compliance with DoD, DISA and DMDC standards, policies and procedures at all DMDC managed sites, specifically the DISA DECC at Columbus.

4.3.21 Manage disk space utilization on all servers including monitoring and enforcement of pre-determined user quota limits and provide a weekly Server Disc Space Utilization Report.

4.3.21A Provide access to network shares, directories, files, SharePoint sites, as requested and approved within the helpdesk ticketing system. Verify with end user owners access can be given to requestor.

4.3.22 Define methodology for identifying and managing risks that may affect cost, schedule and performance; evaluate risk to assess and determine potential outcomes; define steps to respond to and mitigate identified risks; present risk mitigation plan with risks identified; and addresses each risk and changes thereto over time.

4.3.23 Maintain a Work Breakdown Structure (WBS) and detailed project plan for all Server projects and brief the stakeholders on progress and constraints monthly.

4.3.24 Support the physical racking, power-on, and cabling of new or relocated servers to successfully integrate the hardware into the DMDC operational environment.

4.3.25 Support the Asset Management process with removing servers from racks, removing and degaussing hard drives, and palletizing equipment in preparation for DRMO during decommissioning.

4.3.26 Implement and configure automated tools to detect and monitor the operations of the applications. Computer Associates (CA) Unicenter is the monitoring and agent component used for the automated monitoring; however, the Government may procure and direct a replacement of this suite during the performance period

4.3.27 Perform normal system operation functions and system console operations using DMDC established processes and procedures. These include:

- System reboots
- System stop/start/resets
- Initial system load using the most current OS image (jumpstart/kickstart)
- Load/unload of configuration media
- Functions required as a part of server decommissioning, including disk erasure
- All functions requiring root-level authority

4.3.28 Detect and monitor operations of applications using CA Unicenter or like product. A list of elements monitored for each server is provided in the Appendices. Performance monitoring will be facilitated with Team Quest and VMWare vCops

4.3.29 Track all incidents from problem identification through problem resolution with primary focus on immediate service restoration to minimize impact to user community.

4.3.30 Analyze data storage requirements and design appropriate backup strategies, processes, and procedures for all networked systems.

4.3.31 Ensure appropriate coordination and flow of information among all necessary parties including help desk support personnel to quickly restore service availability, minimize service disruptions, and respond to customer needs by using existing incident and service request management tools.

4.3.32 Perform Server Administration support for the day-to-day management and sustainment of the server environment to include hardware, operating environment, utilities, communications application and executive software, and software support necessary for managing the computer's resources, file structures, procedures, performance, and capacity.

4.3.33 Administer Windows operating system security in accordance with published DoD security standards (Security Technical Implementation Guides (STIG), IA Vulnerability Management (IAVM), Vendor released patches, Higher level Directives and Federal/DoD/DISA policy for vulnerabilities and system patches to ensure server security posture.

4.3.34 Ensure current software version and release levels are installed and changes follow DMDC change management processes.

4.3.35 Ensure appropriate coordination and flow of information among all necessary parties including help desk support personnel to quickly restore service availability, minimize service disruptions, and respond to customer needs by using existing incident and service request management tools.

4.3.36 Update and maintain a Standards and Procedures Manual for performing system administration.

4.3.37 Monitor and control storage performance according to technical standards & Specifications, Storage and Data Management policies & procedures, and perform tuning as required.

4.3.38 Request for changes to the environment at this site must be approved by Government technical team and must originate via a change request.

4.3.39 Conduct the implementation and operation of the backup jobs and routine maintenance of the Net Backup subsystem. Provide tape backups and restores for disk storage devices. This includes daily incremental and weekly full backups across the installed base of servers and databases

4.3.40 Provide input to after action report and participates in conference calls.

4.3.41 Work with building facilities team to ensure, sufficient power and cooling.

4.3.42 Maintain documentation of rack elevations to expedite placement of new equipment using GFE (i.e. Netzoom, StruxureWare).

4.3.43 Execute tasks from Project Change Requests and associated child Change Request and child Requests.

4.3.44 Process new hardware when received. This will require contractor to unpack, rack, power, network and console connectivity. Coordinate with vendors for installation and initial training. Racks and individual servers marked front and back. Decommission checklist including un-rack and assist asset manager with DRMO.

4.3.45 Bulk email distribution

4.3.45.1 DMDC manages its own email service for bulk email distribution (currently Strong Mail). DMDC is in the process of identifying a follow on bulk email distribution solution. The server team will manage the bulk email service solution to include maintenance, patching and updating, conflict resolution and problem troubleshooting and repair.

4.3.45.2 Server team will also manage DMDC's SMTP relay service, which the bulk system is dependent on. The SMTP relay service is a Microsoft IIS service. The team should have expertise with Microsoft's IIS service.

4.3.45.3 The server team will be required to have regular interaction with DISA's EEMSG team to resolve issues with bulk email leaving the DISA NIPRNET.

4.3.46 Non-Security Patch management

4.3.46.1 On occasion, vendors release patches for their software that are not considered security patches, but product enhancements or bug fixes. The contractor will review different patches released by vendors, for both OS and software implementations, and make recommendations to the Government as to which enhancing, non-security patches should be applied to software and OS installations. The contractor will submit a change request to the change request system as their recommendation. Upon Government approval through the change request system, the contractor will apply approved patches via regularly scheduled maintenance.

4.3.47 Secure Operation Centers

DMDC has Secure Operations in multiple locations (Seaside, CA, Cheyenne Mountain, CO, Boyers, PA and the National Capital Region).

a. Capability Requirements – The contractor shall:

4.3.47.1 Responsible for all aspects of operating, maintaining and sustaining the DMDC classified environment to ensure robust performance, reliability, availability and scalability at a Mission Assurance Capability (MAC) 1 like Classified Level.

4.3.47.2 Provide all aspects of operating, maintaining and sustaining the DMDC classified environments to ensure robust performance, reliability, availability and scalability at a Mission Assurance Capability (MAC) 1 like Classified Level.

4.3.47.3 Provide all aspects of managing the security to include: access control systems & methodology, development, business continuity planning, operations security, physical security, security architecture & models and security management practices for all database infrastructure systems and the underlying operating system.

b. Subtasks:

4.3.47.4 Maintain and enhance clear and concise documentation and diagrams for processes, policies and procedures for all areas of responsibility including; standard operating procedures, hardware inventory, license management, problem escalation, disaster recovery, network topography, and network operations.

4.3.47.5 Maintain the software and database servers on existing and future server hardware and COOP servers.

4.3.47.6 Monitor, configure, and optimize the system; add, modify, and remove user access to the system.

4.3.48 Storage Operations / Functions

Managing the disk storage arrays, storage area network and tape robot systems within DMDC. Responsibilities include developing a storage management program, firmware patching for the entire SAN fabric, arrays and server HBA's, LUN layout for SAN and NAS for all models and makes that are within the DMDC enterprise like NETAPP, HITACHI, HP EVA, SPECTRA LOGIC, BROCADE and NIMBLE etc.

a. Capability Requirement – The contractor shall:

4.3.48.1 Provide employees with an IT1/ADP-level vetting to support the DMDC Storage Area Network (SAN) disk storage Configuration Management .

b. Subtasks:

4.3.48.2 Get prior approval from the Government to make changes to the DMDC SAN.

4.3.48.3 Provide Problem Management support for storage array and fabric.

4.3.48.4 Open a Service Request with the storage appliance maintenance vendor for error conditions and to ensure proposed configuration/microcode upgrades are vetted by their engineering staff.

4.3.48.5 Execute all volume assignments vetted through Change Request process of DMDC storage resources.

4.3.48.6 Maintain DMDC's storage configuration documentation.

4.3.48.7 Control access to SAN management resources, by restricting IDs, passwords, functionality, and IP addresses, to individuals directly supporting the resources.

4.3.48.8 Configure and create zones to establish a link between server Host Bus Adaptors and Fiber Adaptors. Incorporate and maintain the use of a fabric director for the data integrity of the DMDC environment.

4.3.48.9 Provide recommendations for further tuning or optimization.

4.3.48.10 If workload increases or capacity issues exist, the additional capacity required, supporting this growth and resolving capacity-related issues will be the responsibility of the storage administrators, in conjunction with IT OPS management.

4.3.48.11 Recommend new technologies to the Government to keep abreast of advances in commercial technologies

4.3.49 Cluster Management

Manage all the different types of hardware and software clustering within DMDC's enterprise, including but not limited to those indicated below. Install or uninstall cluster software, configure and administer cluster software packages. Apply cluster software patches, hotfixes, and service packs. Maintain Operational Procedures documentation for cluster operations. Types of clustering include but are not limited to, SYMANTEC VERITAS HA, ORACLE RAC, MICROSOFT CLUSTERING, VMWARE HA, etc.

a. Capability Requirements – The contractor shall:

4.3.49.1 Perform Cluster Management activities using various cluster technologies.

- all aspects of installing/uninstalling the software
- configure and administration to include startup and shutdown)
- applying software patches
- hotfixes and services packs
- maintaining operations procedures documentation
- root cause analysis
- Coordinate problem resolution activities

4.3.49.2 EXADATA

Exadata is an Oracle engineered system.

a. Capability Requirements –The contractor shall:

4.3.49.2.1 Data Base Administrators and UNIX sysadmins will be required to work together to manage the Exadata HA, replication, storage cells and database compute nodes as a whole integrated system.

4.3.49.2.2 Exadata requires close management and coordination among various IT Operations groups and Oracle Exadata team.

4.4 TASK 4 – Perform Network & Telecommunications Management

The Network/Telecommunication administrators are responsible for the day-to-day operations and maintenance of the DMDC Enterprise Network and Telecommunication infrastructure. The administrators carry out responsibilities in some or all of the following technical areas: hardware and software maintenance, system upgrades, infrastructure design and layout, disaster recovery design and implementation, monitors, software patching, maintains DoD and DMDC security policies and, troubleshoot; train and or supervise staff; or offer technical support for projects.

There are two cross domain environments at DMDC, one at Seaside, CA and the other at Colorado Spring, CO. The network team is responsible for the network connectivity, maintenance, and patching of the supporting network equipment at the new locations.

a. Capability Requirements – The contractor shall:

4.4.1 Monitor, administer, securely install, configure, and maintain network equipment such as routers, switches, firewalls, IA Security encryption devices, load balancers, DNS appliances, and network interface cards. This shall be performed on the DMDC Unclassified Data Network (NIPRNet), and the Classified Data Network, (SIPRNet) in accordance with Department of Defense (DoD), DMDC regulatory guidance and compliance standards and, when applicable, with the International Standards Organization (ISO) recommendations with service availability of 99.9%.

4.4.2 Identify, isolate, troubleshoot, correct and document any/all problems within the DMDC Network and Telecommunication Infrastructure to include the Wide Area Network (WAN), Local Area Network (LAN), Enterprise Firewalls/Routers/Switches, Load Balancers, DNSSEC, PBX/VOIP and Remote Access Service (RAS). 802.1x, NAC/NAP, Manage, operate, and support the Virtual Private Network (VPN) access and gateways to include user-access requirements.

4.4.3 Provide, secure and maintain optimally configured telecommunication resources to support the DMDC Enterprise at all sites. Support includes integration, installation, upgrades, decommissioning, patching and service availability, and coordination with DoD network and telecom providers. (See Appendices)

4.4.4 Monitor all Network & Telecommunication Infrastructure equipment to include circuits, nodes and hardware supporting the Enterprise (See attached Inventory list in Appendices).

4.4.5 Securely rack, install, cable, configure, and maintain network and telecommunication infrastructure resources such as routers, switches, (Juniper, CISCO and Brocade Data Storage switches), firewalls, IA Security Devices, web proxies, F5 load balancers, Global Traffic Managers, and network encryption devices, and PBX/VOIP resources. This is applicable to current Network

and Telecommunication Infrastructure Assets and future environments including emerging technologies.

4.4.6 Monitor status of all network devices and communication circuits and ensure all firewall rules incorporated strictly adhere to DoD Ports and Protocols Service Management (PPSM) guidelines.

4.4.7 Provide complete lifecycle support for DMDC enterprise network assets and configurations. Ensure all approved network components are integrated and operate in accordance with OEM performance standards. Every effort must be taken to ensure the maximum amount of operational availability of network services.

4.4.8 Perform all network device administrative functions. All administrative operations shall be performed in a manner in which adverse impact on network availability is minimized and in accordance with established standard operating procedures.

4.4.9 Perform all security configurations and operations in accordance with the DoDI 8500.2 and compliant with any additional DoD Instructions, US CYBERCOM Orders, Federal Information Security Management Act (FISMA) and DMDC policies.

b. Subtasks:

4.4.10 Review and validate all telecommunications circuits and formulate recommendations for retention, cancellation or transfer of responsibility.

4.4.11 Maintain a real-time database of the installed equipment detailing: equipment descriptions, serial numbers, quantities, locations, maintenance levels, circuit IDs and inventories, and Point-of-Contacts as well as tracking all network router installations to include equipment descriptions, serial numbers, quantities, locations, maintenance level, and circuit inventories.

4.4.12 Optimize performance, perform system station back-ups on a weekly basis, and recover, configure and connect hardware.

4.4.13 Develop, propose, and implement plans for continual availability improvements for the network and telephony services and administer availability of telephony infrastructure. Support telephony requests and incidents.

4.4.14 Respond to receipt of a notification of outages, disruptions or failures within 10 minutes.

4.4.15 Maintain an accurate Cabling to Network Switch port inventory ensuring any and all changes deployed in Data Centers (Primary and Secondary), and remote sites are updated within 5 business days. This is to provide an up to date inventory or documented mapping of all cable runs to network switches to aid and assist in any troubleshooting efforts.

4.4.16 Monitor and report on the overall health of the system infrastructure, to include equipment attached to the network and all applications directly supporting the network. Support shall include interacting with DISA to provide technical assistance via phone or e-mail.

4.4.17 Scheduled VOIP outages will be approved by the Government and adhere to IT OPS Standard Operating Procedures to ensure visibility and proper coordination.

4.4.18 Troubleshoot and resolve all LAN/WAN issues. Devices to be administered include:

- Firewalls
- Switches
- Routers
- Virtual Private Network appliances
- Load Balancers
- Hardware Security Modules
- Secure Socket Layer (SSL) accelerators
- On-line Certificate Status Protocol (OCSP) servers
- Host/Network Intrusion Detection Devices
- IA Security Devices
- Network management software that is part of the interface between the administrator and the network appliances
- IP Phones
- 802.1x/Certificate Authorities – To meet DoD regulations, DMDC must employ IEEE 802.1X Network Access Control across the DMDC Enterprise (NIPR and SIPR).
- Network Access Protection (NAP) – Standup and maintain a Government approved NAP infrastructure using DMDC provided Information Assurance software.
- Network Access Control (NAC) - Standup and maintain a Government approved NAC solution to authenticate DMDC workstations using certificates derived from a DMDC controlled Certificate Authority.

4.4.19 Develop and present for approval implementation plans for continual availability improvements of network services and track change management activities that impact network administration functions.

4.4.20 Conduct device firmware patches, OS patches, device configuration file changes, device installation, decommission and support for issues related to network devices and servers to support VoIP within the DMDC enterprise enclave.

4.4.21 Implement and maintain security configurations for all DMDC enterprise network assets and configurations. All security configurations and operations will be in accordance with the DoDI 8500.2 and compliant with any additional DoD Instructions, US CYBERCOM Orders, Federal Information Security Management Act (FISMA) and DMDC policies. The cybersecurity branch will detect any deviations as part of regular scanning and auditing. The contractor must respond to any issues with either a fix or adequate justification for non-compliance which is accepted and approved by our cybersecurity staff. Additionally, the contractor should be proactive and coordinate any non-compliance issues in advance of identification by the cybersecurity team. Failure to apply any STIG configuration setting must be approved by the Cybersecurity Branch.

4.4.22 Perform network cabling. This includes management of the cabling between network devices and servers, cablings from the network operations centers to the wall plates and connectivity from the wall plates to the end-user workstation.

4.4.23 Support secure and non-secure voice networks consisting of user telephone instruments, Secure Telephone Equipment (STE) instruments, and voice-over-IP (VoIP) network and instruments. The contractor shall provide onsite troubleshooting, problem isolation, and service restoration.

4.4.24 Coordinate maintenance and repairs with vendors per published schedules or when necessary, due to hardware or software failures.

4.4.25 Provide and monitor remote teleworker access and performance. Recommend changes and technology upgrades which will improve performance for remote access customers.

4.4.26 Support the physical racking, power-on, and cabling of new or relocated servers to successfully integrate the hardware into the operational environment.

4.4.27 Support the Asset Management process with removing servers from racks, removing and degaussing hard drives, and palletizing equipment in preparation for DRMO during decommissioning.

4.4.28 Address and remediate vulnerabilities identified in Assured Compliance Assessment Solution (ACAS), DMDC/DoD vulnerability management tool managed by Cybersecurity Branch.

4.5 Task 5 – Conduct Virtualization Administration

The Virtualization Administrator is responsible for the day-to-day operations and maintenance of the Shared Services Virtualization servers and infrastructure. The Virtualization Administrator carries out responsibilities in some or all of the following technical areas: hardware maintenance, system upgrades, infrastructure design and layout, disaster recovery design and implementation, hypervisor installation and maintenance, Site Recovery Manager Deployments, physical to virtual migrations, and hypervisor server hardening.

a. Capability Requirements – The contractor shall:

4.5.1 Maintain current industry knowledge of development concept, practices, and procedures. Must possess experience in Enterprise Data Centers; demonstrated knowledge and experience with virtualization technologies for Data Center Virtualization, Cloud based computing, and End User Computing (i.e. VMWare, Citrix, et.).

4.5.2 Develop an in-depth understanding of the active Virtual IT baseline capabilities, design, and objectives.

4.5.3 Provide technical operating system documentation, trained users in applications and operating system fundamentals for the entire DMDC virtual infrastructure.

4.5.4 Cloud Management intends to build upon the core foundation of virtualization to introduce new abstraction layers through software to increase agility through automation. In addition, the introduction of a self-service multi-tenant model is critical, all the while being fully secure and in compliance (e.g., DISA STIG or DMDC Compliance baseline).

b. Subtasks:

4.5.5 Provide for implementation, troubleshooting support, maintenance and capacity planning of the Virtualized computing environment including: day-to-day operations, monitoring and problem resolution for virtual environment issues and problems.

4.5.6 Monitor virtualization systems and storage; proactively address or escalate issues before service is impacted; provide Tier II problem identification, diagnosis and resolution of problems in the virtual environment.

4.5.7 Maintain O&S standard operating procedures for the virtualization environment and diagnose and troubleshoot problems with the virtualization environment, including Microsoft, UNIX and Linux O/S.

4.5.8 Support off-hour maintenance activities and support the certification and accreditation process for virtualization hosts.

4.5.9 Establish and maintain monthly patching for all virtual systems and evaluate patches before installation utilizing the tool sets provided for the virtual infrastructure.

4.5.10 Work with the different business units to develop the engineering design to support the business and operational requirements for either new systems or enhancements to existing systems. Interact with the project engagement.

4.5.11 Define standard engineering designs, templates, processes, and procedures for implementing projects that follow existing DMDC virtual architectures.

4.5.12 Analyze system performance, modifying parameters to improve throughput and effectively utilize system resources. Monitors resource usage, making required adjustments utilizing tools like VCOPS and TeamQuest.

4.5.13 Manage all virtual infrastructures i.e. VMware, VDI, Citrix, SRM replication, Oracle LDOMS and zones, hardware virtualization and Infrastructure Operations.

4.5.14 Manage and support blade chassis and all associated components as it relates to virtual technologies and OS deployments.

4.5.15 Participates in on-call production support activities 24 X 7 X 365. Requires technical knowledge and capability to handle all problems that may arise within a virtual environment. Proactively put procedures in place to prevent and reduce the severity of outages. Implement automation wherever possible.

4.5.16 Architect an industry standard virtualization layer that includes the following domains: Compute, Storage, Network, Operation System, High Availability/Fault Tolerance, Disaster Recovery and Application Dependencies which resides in the Management domain.

4.5.17 Implement VMware vCenter Chargeback Manager (vCBM) to properly bill departments for the resources they utilize.

4.5.18 Provide a plan for the upgrade, expansion or replacement of the current DMDC Virtual Desktop Infrastructure that focuses on the following critical success factors:

4.5.18.1 Have ability to scale in size for future growth of virtual servers and desktops.

4.5.18.2 Centralized management for corporate and personal device options, providing a reduction in hardware and maintenance cost

4.5.18.3 Migration of 500 users to the new solution within 180 days of completion of infrastructure, to include user data back up and transfer, application readiness, and remotely accessible. By end of the base year, preparation for the infrastructure to handle migration of the entire population must be complete.

4.6 Task 6 – Conduct Web Middleware Administration

DMDC maintains a complex web infrastructure with high-availability requirements. The current components of the web infrastructure are indicated in the Appendices. This configuration supports internal as well as external end-user and system to system interfaces for DMDC's service offerings. Support future web infrastructure components at an estimated rate of 10% annually.

a. Capability Requirements – The contractor shall:

4.6.1 Provide the overall administration and maintenance of existing and the creation of new middleware components and engaged in all aspects of middleware administration including architecture, design, configuration, tuning, monitoring, troubleshooting, installation, upgrades, deployment to various environments.

4.6.2 Provide technical expertise and support to other staff members on implementing and integrating middleware products and platform. Provide design and implementation plans for ALL new web or application specific projects that come to IT Operations division.

4.6.3 Adhere to security and operational parameters and constraints existing at the time the integration is required. Administer operation of batch applications.

4.6.4 Provide maintenance and sustainment for all existing and creation of new application servers; application server is a server which provides Java Virtual Machine hosting services to J2EE based application beyond those available from the operating system. (See Appendices for existing servers). A 30% growth rate is anticipated.

4.6.5 Serve as primary escalation point for failed or non-functioning J2EE application deployments in all environments. Currently there are approximately 300 applications supported.

b. Subtasks:

4.6.6 Ensure that middleware infrastructure that supports enterprise applications is scalable and robust to meet current and future provisioning needs. This includes configuring clustered environments as well as disaster recovery solutions.

4.6.7 Provide pro-active monitoring of individual components and the overall middleware products.

4.6.8 Create roadmaps and provide technical architecture thought leadership involving middleware technologies to management.

4.6.9 Implement and manage effective backup/archive strategies for middleware environments. Perform backups, restores and disaster recovery functions including disaster recovery drills.

4.6.10 Document existing and new middleware platforms and infrastructure with respect to functionality, maintenance and administration. Keep this documentation in a centrally located place accessible to all relevant team members.

4.6.11 Provide support for the administration of web server applications. Administration tasks include: integration, installation, upgrades, decommissioning, patching, etc. and performing tasks to maximize web service availability and conformance to DMDC and DoD policy.

4.6.12 Plan, test, and implement initiatives to incorporate new technologies not currently present within the DMDC web environment.

4.6.13 Develop implementation plans for continual availability improvements of web services and submit for Government approval 90 days after contract award.

4.6.14 Support project planning of new projects with the customer base.

4.6.15 Stay abreast of industry trends and all applicable technologies, including scripting, security issues, authoring tools, graphic design tools, and new languages.

4.6.16 Analyze web site traffic and recommend programming changes; manage transfer of files and memory allocation for web site on the server.

4.6.17 Maintenance

4.6.17.1 Test and apply IAVM patches and remediation before the date given in the IAVM alert. Comply with IAVM reporting procedures.

4.6.17.2 Maintain a mounted file system installation shared across all respective environments (Production, Contractor Test, Stress Test, Quality Assurance, Development Test, etc.).

4.6.17.3 Perform log analysis, error detection, and fault correction on all web servers

4.6.17.4 New Server Builds

4.6.17.4.1 Build and confirm functionality of Web Servers within 2 weeks of request. Web Servers will be built according to STIGS, patched and approved for production use by Cybersecurity Pre-production Scanning Process.

4.6.17.4.2 Create and remove systems hosted Uniform Resource Locator (URL) addresses. For new secure and non-secure URLs created on web servers they will be configured and functioning within 1 month of the request date and conform to DISA standards for URL security.

4.6.17.4.3 Complete a migration of Production Web Applications within the systems enclave to bi-locational single URL address (1 app per URL) and support the ongoing transition of the remainder within the established project timeline.

4.6.17.5 Application Servers

4.6.17.5.1 Test and apply mandated IAVM patches and remediation before the date given in the IAVM alert. Comply with IAVM reporting procedures.

4.6.17.5.2 Maintain a mounted files system installation of WebLogic shared across the respective environments (Production, Contractor Test, Stress Test, Quality Assurance, Development Test, etc.).

4.6.17.5.3 Perform log analysis, error detection, and fault correction on all application servers. Servers will be built and functioning within 2 weeks of request and will include only the enterprise version of Oracle WebLogic via shared file systems and will not utilize local storage. Oracle WebLogic configuration will be 100% consistent with current Production application servers.

4.6.17.5.4 Build application servers according to STIGs, patched and approved for production use by Cybersecurity Pre-production Scanning Process.

4.6.18 Deployment Support

4.6.18.1 Assess all failed or nonfunctioning deployments and prepare for redeploy within a single working day for Production or 3 days for non-production environments (Contractor Test, Stress Test, Quality Assurance, Development Test, etc.).

4.6.18.2 Responsible for "first time setup" on newly deployed applications within the WebLogic environments. This includes:

- Domain initialization and configuration
- Managed Server initialization, configuration, and clustering
- Listener context root configuration

4.7 TASK 7 – Database Administration

Database administration is the function of managing and maintaining database management systems (DBMS) software. DBMS software such as Oracle, SYBASE, IBM DB2 and Microsoft SQL Server need ongoing management or high level administration. DMDC Systems DBA's focus on the physical aspects of database administration such as DBMS installation, configuration, patching, upgrades, backups, restores, refreshes, performance optimization, maintenance and disaster recovery.

a. Capability Requirements – The contractor shall:

4.7.1 Provide database administration support for the current enterprise DMDC operating environments to include Oracle (version 11g or higher), MS SQL (version 2008 R2 or higher), Sybase Adaptive Server Enterprise (version 15.0 or higher), NoSQL, Hadoop and MySQL platforms.

4.7.2 Develop technical specifications, design, develop, modify, test and manage databases in DMDC's multi-tier application architecture. Monitor and optimize database performance and tune database operations. Ensure that data integrity facilities for databases are executed and that application developers are aware of any anomalies.

4.7.3 Ensure that applications, interfaces, extensions, forms, and reports integrate with database architectures.

4.7.4 Administration of database, storage management, high availability and replication like ASM, RAC, DataGuard, SymetricDS and GRID technologies.

4.7.5 Understanding and be able to work with various operating system environments.

4.7.6 Understand Disaster Recovery requirements and processes.

4.7.7 Understand capacity planning as it pertains to databases.

4.7.8 Be able to administer Oracle EXADATA Database systems.

4.7.9 Assess, Design, Deploy, and Operationalize DMDC's mission critical workloads that are currently being supported by all databases

b. Subtasks:

4.7.10 Perform reverse engineering when database corruptions occur or as a result of troubleshooting systems and restore databases to uncorrupted versions.

4.7.11 Provide detailed technical direction to application developers and stakeholders who have been assigned to assist with modifications or changes to the computer programs involved.

4.7.12 Deliver implementation plans that provide the detailed approach taken when implementing new database features, versions, and/or capabilities. Define and administer quality control methods, and drafts detailed and comprehensive documentation covering user requirements, system design, new software, and software modifications.

4.7.13 Create and test backups of data, provide data cleansing services, verify data integrity, implement access controls.

4.7.14 Develop implementation plans for continual availability improvements of database services. Every effort must be taken to minimize unavailability of the database services.

4.7.15 Develop, manage and support the SQL databases used for the DMDC Web, SharePoint sites, portals, and supporting SQL databases. Provide technical guidance and advice to division Webmasters.

4.7.16 Provide application deployment support, analysis for performance improvements in procedure or application processing flow, automated scheduling, and statistical trends.

4.7.17 Create and maintain run books that define standard operating procedures for all provided services for setup and configuration of applications, deployments of applications, application startup order of dependencies, and health-monitoring requirements to ensure availability.

4.7.18 Engage with database vendors to validate and deliver a plan of action that will take DMDC from its current state to the proposed future architecture in alignment with DMDC's strategic plan (fit into DMDC future direction)

4.7.19 Implement Log Management security correlation engine to protect DMDC from external threats such as bots, worms, and internal risks such as fraud and theft.

4.7.20 Monitoring and optimizing the performance of all DMDC databases

4.7.20.1 Planning for backup and recovery of database information

4.7.20.2 Maintaining archived data on tape

4.7.20.3 Backing up and restoring the database

4.7.20.4 Contacting all database vendors for technical support

4.7.20.5 High availability administration (RAC), backup, recovery, performance tuning and troubleshooting of production, DR and test RAC databases.

4.7.21 Creates and supports databases across internal and end-user applications, improve database integrity through quality assurance and manage change control processes related to the Oracle environment.

4.7.22 Analyze, test, coordinate and facilitate patching needed to maintain PCI compliance.

4.7.23 Analyze existing database applications for improvements, database tuning & monitoring, working with application developers to integrate efforts with relational databases, participate in team or company projects as required, maintain state-of-the-art knowledge of existing best practices in database administration, mentor/train lower level database administrators, perform all tasks associated with disaster recovery exercises, capacity planning and able to provide 7 x 24 hour on-call support any day of the week.

4.7.24 Develop and troubleshoot shell scripts as needed.

4.7.25 Ensuring RMAN and backup processes and procedures are followed and maintained.

4.7.26 Provide monthly database utilization reports and configure scripts where necessary to manage/provide notification of database thresholds.

4.8 TASK 8 – Provide Help Desk Services

DMDC IT Operations Enterprise Helpdesk is responsible for providing basic application software and/or hardware support to callers. Help Desk represents the "customer facing" component of the IT Operations Division by serving as a portal and conduit for all DMDC customer inquiries. Help Desk responds to inquiries pertaining to the DMDC information technology infrastructure such as hardware, software, user account security, communications and IT Operations policy guidance to end users. Some of the support and services provided include DMDC Information Technology (IT) infrastructure which includes; desktops, laptops, software; printers; document scanners; audio-visual equipment/VTC; handheld devices; network service outages/disruptions; and enterprise server outages/disruptions. Operate a Tier level-one, consolidated customer help desk to serve as the single point of contact (POC) to answer IT/IM trouble calls for approximately 1900 end users.

a. Capability Requirements – The contractor shall:

4.8.1 Operate a level-one, consolidated customer help desk serving as the frontline in supporting DMDC's information technology. Help desk staff shall be trained in preliminary diagnostics and resolution of common user Incident/Problems. The key high-level objectives are to improve customer service, problem resolution-speed, and end-user self-service abilities.

4.8.2 Adopt knowledge databases and best practices in the areas of customer reporting, logging, tracking, resolving of IT problems and service requests

b. Subtasks:

4.8.3 Improve efficiency and effectiveness by early identification and addressing root causes of technical problems including working with specialized entities for resolution before they become trends

4.8.4 Monitor all help desk tickets, ensuring tickets are documented concisely and closed within timeframes for routine, regular, urgent, critical and emergency 95% of the time.

4.8.5 Maintain and update Checklists and/or Scripts in high focus Incident/Request areas ensuring continuity with all Help Desk personnel at the Mark Center and DoD Center Seaside.

4.8.6 Upon receipt of a customer's trouble-call, perform the required assessment, utilizing remote access, troubleshoot, isolate and resolve, or refer to the next tier level of help.

4.8.7 Perform predictive analysis to anticipate changes in call volume (i.e. major evolution of software).

4.8.8 Respond promptly to user calls for assistance, giving first priority to staff work stoppages.

4.8.9 Add, set up, and delete user accounts, unlock accounts when appropriate.

4.8.10 Develop a weekly status report of all help desk tickets and the progress of resolution efforts.

4.8.11 Notify the Government of all work requests that take longer than 24 hours to resolve in a daily (Monday through Friday) exception report. If requests require hardware or software that is not currently available, notify the Government as soon as the shortfall is identified. Notify Government of tickets classified as urgent or above.

4.8.12 Staff the help desk from 0700 to 2100 hours (EST), Monday through Friday. Staffing should be split between DMDC, Seaside, CA and Mark Center, Alexandria, VA. Staffing should be based on expected need and adjusted to maintain acceptable performance.

4.8.13 Document all tickets using the current Incident, Request, Problem and Change Order categories to capture category/volume.

4.8.14 DoD Enterprise Email (DEE) Support

The DoD Enterprise Email (DEE) service provides secure cloud-based email to DMDC. DEE provides a Level II, Tier II service desk to an organization's Level I, Tier II and III end user support. DEE service desk will coordinate with an organization's service desk to resolve incidents and problems related to DEE should they arise. DISA integrates DMDC into the operational structure and provides 24x7x365 support through a central service desk.

4.8.14.1 Provide Tier I and II support for email services provided by DISA. Tier I support will be thru the DMDC helpdesk and will collect information regarding DEE. Upon receipt of a call, the helpdesk will log a ticket describing the issue, attempt to resolve the issue or route the ticket to the Desktop Tier II support team. Tier I support will also be the primary team creating and maintaining user accounts, non-personnel entities (NPE) and distributions lists for DMDC using DISA's Defense Enterprise Provisioning Online (DEPO) online service, Outlook Web Access (OWA) and possible other tools as they become available.

4.8.14.2 Assist all users with issues related to the Outlook client, user's workstation and network connectivity within DMDC's enclave. If it is deemed the issue is not with the end user's Outlook or workstation configuration, or DMDC's network enclave, Tier II will transfer the ticket back to DMDC's Tier I Helpdesk. At that time, Tier I will contact DISA's Tier I helpdesk staff to have a ticket generated with DISA on behalf of the user. Once a DISA ticket is created, DMDC's helpdesk staff will add the DISA ticket number to the DMDC helpdesk ticket number for cross reference purposes. DMDC's Tier I and/or II staff will then remain the primary point of contact on the end user's behalf with DISA's staff to resolve the issue.

4.8.14.3 Interface with DEE Helpdesk regarding Exchange Mail Systems.

4.9 TASK 9 – Support End Users Devices & Peripheral Administration

The scope of this task is to provide end user device services and support to DMDC users located at the Headquarters office in the National Capitol Region as well as other locations (See Appendices), remote users and alternate work locations. DMDC may choose to add additional locations and users over the course of this contract. DMDC infrastructure includes approximately 3000 desktop PCs, 500 laptops and 250 handheld devices (blackberry's, smartphones, tablets). Approximately 2000 PCs are located in Seaside, CA and approximately 1000 PCs are located at the different sites across the continental United States. DMDC refreshes approximately 1/3 of their PCs yearly. For a complete listing of peripherals see Appendices.

a. Capability Requirements – The contractor shall:

4.9.1 Conduct testing, implementation and administration of Operating System patches and upgrades approved for use by the Government. This includes the application of all required security patches, version upgrades, security lockdowns and installation of approximately 60 new or upgraded applications per year to some or all users. Historically 75% of the software is distributed remotely.

4.9.2 Manage the lifecycle of all software and ensure that no user licenses related to supported applications expire.

4.9.3 Support workstation operating system upgrades according to industry requirements minimizing impact on the productivity of the workforce.

b. Subtasks:

4.9.4 Manage the lifecycle of all software approved for use on end user devices. This includes evaluation and integration testing of proposed software packages, delivery and installation of software and upgrades or patching of currently supported software packages.

4.9.5 Notify the Government of major upgrade requirements due to vendor end-of-life announcements and provide an upgrade plan to minimize customer impact. Remove obsolete software from computers.

4.9.6 Maintain the current baseline image and create additional standard images that can be utilized on multiple hardware platforms. Perform maintenance to the baseline image for operating system and application updates to include security patches, hot fixes, application update and upgrades and any additional enterprise software. Baseline images, both desktop and server images, should be updated with latest patches and security updates. DMDC currently supports two (2) Windows 7 desktop images.

4.9.7 Provide support for the administration of all physical and virtual workstations, mobile computing devices, peripheral devices and end user software applications which support on-site and telework workforce in both the classified and unclassified environments.

4.9.8 Resolve end user incidents related to on-site software or hardware and fulfill approved end-user requests for software, hardware or configuration changes in accordance with DMDC governance rules.

4.9.9 Plan, analyze and resolve end user incidents related to on-site software or hardware, remote access infrastructure and mobile devices.

4.9.10 Plan, analyze, troubleshoot, integrate, install, test and validate, operate, maintain, train, document, and provide administration services for all desktop hardware and software systems.

4.9.11 Perform IT equipment relocations, new equipment delivery and installations in support of office moves.

4.9.12 Audio Visual/Video Teleconference Support

DMDC supports various sites with Video Teleconference (VTC) capabilities. DoD Center, Seaside, CA (includes one classified VTC) and the Mark Center, Alexandria, VA and between these two sites they have nine (9) rooms with Video Teleconference (VTC) capabilities. Additional VTC supported sites are: Defense Human Resources Activity (DHRA) Headquarters office, Personnel & Readiness Information Office (P&R IM) and Defense Manpower Data Center, Beauregard located in Alexandria, VA, as well as, Defense Manpower Data Center-TVPO, Arlington, Virginia and Defense Manpower Data Center - JAMRS, Crystal City, Virginia (schedule to move to Mark Center, July 2015).

a. Capability Requirements – The contractor shall:

4.9.12.1 Troubleshoot (at Tier 2 Level) computer and Tandberg equipment ensuring, audio, video integration are in a fully operational state.

4.9.12.2 Perform preventative maintenance such as replacing lamp bulbs, cleaning filters, cabling integration with computer systems.

b. Subtasks:

4.9.12.3 Maintain internal connectivity for NIPR and SIPR VTC connections within the DMDC Enterprise via switches, routers and firewalls and other controlling factors.

4.9.12.4 Provide Tier 2 support for Town Halls and other high level meetings, including DCS (formally DCO) and VTC.

4.9.12.5 Tier 2 will provide troubleshooting and document all VTC support incidents; if it cannot be resolved at Tier 2, then it is escalated to the vendor for Tier 3 support.

4.10 TASK 10 – Provide Systems Build, Integration & Testing Environment

The DMDC IT Support Division was tasked with consolidating several distinct computer labs into a single, agency-wide, integration & testing environment, capable of supporting myriad IT systems, projects, and environments (physical and virtual), through their planning, development, testing, quality assurance, and deployment phases.

a. Capability Requirements – The contractor shall:

4.10.1 Assist with the modernization and daily operation of the integration & testing environment, to include: workstation (desktop, laptop, tablet, smartphone) analysis, administration, testing and security; server (physical/virtual) analysis, administration, testing and security; network (wired/wireless) architecture analysis, administration, testing and security; COTS/GOTS approved open source software analysis, administration, testing and security, to include deployment capabilities; Voice-over-IP (VOIP) technologies analysis, administration, testing and security; and other new technologies.

b. Subtasks:

4.10.2 Document the activities required to install the necessary components and describe how components will be synthesized into an integrated system.

4.10.3 Develop installation, integration, and test plans for implementation of new applications. Test and diagnose system performance and document testing results. Coordinate with proper teams to modify/update systems according to the results, enhancing system performance and repairing application abnormalities. These plans shall be incorporated into a project management plan and briefed to key stakeholders.

4.10.4 Propose methods or architectures allowing lab networks to communicate with needed production IT services while posing a manageable technical risk to the production environment.

4.10.5 Prepare and exercise testing scenarios to verify the operations stability of new hardware and software prior to its use.

4.10.6 Provide troubleshooting on existing hardware and software to isolate and resolve the inevitable problems that occur on operational networks.

4.10.7 Maintain and update test environment architecture and configuration settings to be production like environment.

4.11 TASK 11 – Conduct Mainframe Support Services

DMDC operates an IBM z10 Series Mainframe currently located at the Naval Post Graduate School (NPS) in Monterey, CA. The system provides computational and supports DMDC and other tenant organizations computing and networking services. The mainframe operates up to four Logical Partitions or LPARs. The mainframe consists of one IBM Open System-ZOS production partition one ZOS development partition and one ZOS-ZVM-UNIX-LINUX development partitions, and one IBM ZVM production LPAR.

a. Capability Requirements – The contractor shall:

4.11.1 Provide personnel with extensive knowledge and experience with the installed IBM mainframe system and application software. Majority of work can be performed remotely. Some hands on work will be required onsite. Additionally, personnel shall have expert understanding of IBM's zSeries mainframe, LPAR configuration, and alternative workload structure. Appendices provide a list of the applicable software applications and key components to the system.

4.11.2 Manage the technical life cycle of the z/OS software product, package, or subsystem assigned. This involves the full spectrum of the technical life-cycle of these entities, including: requirements determination, technical design, prototyping, performance prediction/modeling, installation, customization, problem management, documentation, security compliance, change control, regression avoidance, license-key management, single-point-of-failure elimination, recovery automation, and assured availability.

4.11.3 Assist the DMDC in the configuration of Resource Access Control Facility (RACF) Support.

4.11.4 Provide IBM z/OS System programming, maintenance, and configuration support. Third-party systems software installed must be kept compliant with current operating system. New software may be required as a result of customer requests, standardization, or vendor directives.

4.11.5 Monitor functioning of Z10 Mainframe, ensuring that Z10 is running up to standards established by original Equipment Manufacturer (OEM).

b. Subtasks:

4.11.6 Support the working of installed software and firmware including system software, utilities, programming languages, compilers, interactive terminal software, and transaction processing software. Provide technical and engineering support in z/OS operating systems.

4.11.7 Perform trend analysis quarterly on system performance and recommend configuration, and assist in the coordination and planning to schedule system upgrades. Coordination may include DMDC and other Agencies at DMDC's direction.

4.11.8 Conduct analysis, installation and testing of all new software releases

4.11.9 Provide technical and user training to DMDC technical staff and end-users.

4.11.10 Provide technical support for the problem resolution process to resolve errors in systems software and coordinate and transition from one hardware subsystem to another as scheduled.

4.11.11 Perform product installs. Research problems and keep current on available patches, fixes, releases, and life-cycle (going-out-of-support) plans. Track problems turned over to vendors for resolution and escalate attention to the problems where appropriate.

4.11.12 Coordinate with DMDC staff to ensure overall efficiency and effectiveness of the mainframe operation

4.11.13 Provide on-call support including answering questions, troubleshooting, and repair problems 24x7x365.

4.11.14 Perform weekly system backups every Sunday to ensure adequate protection of data in accordance with applicable DoD and DMDC directives. Ensure backup data is archived for a period conforming to DMDC dataset storage naming conventions. Document activities and actions taken in a log. Accomplish backups daily, weekly, monthly, semiannually, and annually. Log should be available to the Government on request. Data restores shall be verified every 180 days. All information assurance appliances and systems will be backed up to ensure proper and expedient service restoral in the event of a system outage.

4.11.15 Perform system control and tape library functions to include: locate and store media; reorganize files as necessary; inform DMDC of input data errors; and schedule due-in or due-out machine workloads.

4.11.16 Provide IBM z/OS System programming, maintenance, and configuration support. Complete 98% of software updates five (5) days after receipt of software.

4.11.17 Conduct ongoing problem reporting/monitoring, status updates, software/hardware incident logs, capacity planning processes and procedures, etc. Update the information on the DMDC ITO SharePoint site weekly.

4.11.18 Coordinate with DMDC and other Agencies at DMDC's direction to ensure overall efficiency and effectiveness of the mainframe operation.

4.11.19 Maintain and utilize an emergency contact list and escalation procedures to resolve abnormally ended jobs. Resolve abnormally ended jobs caused by conditions external to production programs.

4.11.20 Enhance processing capabilities and efficiencies through system tuning and other run-time improvements. Analyze performance metrics and respond proactively to potential problem areas.

4.11.21 Attend monthly meetings of Mainframe Users Group and work with DMDC and other Agencies at DMDC's direction on issues raised in the meeting.

4.11.22 Recycle computer tapes, initialize new ones when needed and retire tapes that are beyond their useful life.

4.11.23 Work with hardware repair personnel to ensure that problems with equipment are resolved.

4.11.24 Perform the following duties for job scheduling technology: install and maintain software, set up RACF security, trouble-shoot user and system problems, train personnel in use of job scheduling technology and automate production jobs and system maintenance.

4.11.25 Perform the following duties for secure data transfer software: install and maintain software, set up security for transfers, configure/change nodes for transfers, trouble-shoot problems and set up new transfers and test new connections.

4.11.26 Assist in the communicate with external agencies and customers to establish the best secure solution for electronic data transfers based on their hardware architecture and software capabilities.

4.11.27 Assist in the creation of login IDs, permissions and updated internal documentation for public IP address, point-of-contact, (POC) names, email addresses and phone numbers of agencies connecting with the Mainframe.

4.11.28 Work with DMDC and other Agencies at DMDC's direction to establish connectivity with outside agencies through the network to connect to the mainframe. Ensure that DMDC and other Agencies at DMDC's direction receives IP address, point-of-contact information and that connectivity testing for both test and production environments between DMDC and outside agencies is conducted.

4.11.29 Assist in the creation of user accounts: assign new accounts, delete inactive accounts, and manage active accounts.

4.11.30 Work with Time Sharing Option (TSO) and Virtual Machine (VM) operating systems with the z/OS environment. Edit, modify and create jobs executing within these environments.

4.11.31 Assist in the creation, changes and trouble-shoot problems with JCL and batch processing jobs within the z/OS environment.

4.11.32 Manage, monitor and diagnose system problems for the z/Series IBM Server for computer operations. Define LPAR specifications.

4.11.33 Participate in the planning and procurement of new systems for hardware and software. Review procedures and technical specifications to determine if requirements needs have been achieved.

4.11.34 Assist in Identify critical IT systems, services and business applications; develop recovery strategy; review onsite and offsite backup policies, procedures and standards; develop, document and maintain recovery plan; prepare SOPs and present information to management.

4.11.35 Review, create, and maintain SOP documentation.

4.12 TASK 12: Mainframe Application Programming (OPTIONAL TASK)

a. Capability Requirement: Contractor Shall:

4.12.1 Work with multiple VM "mini-disks", switching between them in the z/VM environment.

4.12.2 Work with Linux and Unix subsystems within the z/OS environment.

b. Subtasks:

4.123 Automate mainframe batch file processing using VM REXX programming language: Understand and be able to apply the following for each batch file processing step in a specific project: process flow, potential failure points, file dependencies, as well as data access security risks and issues (sufficient to abide by all DMDC security policies).

4.12.4 Design/create/test/implement CMS panels to support the 'manual' execution of ALL batch jobs connected with the project as the alternative method if automation needs to be suspended.

4.12.5 Write/test/implement VM REXX logic to display the screens and allow VM users to 'manually' run the batch processes and to automatically run all batch processes. Create VMSCHEDULED tasks to run the automated processes.

4.12.6 Establish connections for VPN tunnels with outside agencies through DMDC and other Agencies at DMDC's direction. Initiate connectivity between DMDC and other Agencies at DMDC's direction and external customers.

4.12.7 Install and implement z/VM in the VMTEST LPAR.

4.12.8 Assist in the planning and installation of hardware, software, and calculate resource requirements for all VM software.

4.12.9 Meet with Mainframe Accreditation Team to discuss and plan installation of DISA's requirement to implement procedures in the appropriate "Security Technical Information Guide

(STIG)" for z/OS, z/VM and Linux environments. Review Access control (AC), Audit and Accountability (AU), Security Assessment (CA) and Configuration Management (CM) controls.

4.12.10 Plan, design, install, configure, implement, manage, backup and upgrade the z/VM Operating System (for the IBM Enterprise z/Series eServer) and its components in support of the organization's IT architecture. Update and maintain the z/VM System Directories and manage its DASD environment.

4.12.11 Plan, install, configure, customize, manage and maintain Linux on the z/Series Enterprise IBM Server running as a guest on the z/VM Operating System.

4.12.12 Manage Linux physical DASD and implement Logical Volume Manager (LVM) to create logical volume groups and address changing disk capacity needs. Perform the initial setup of users, groups, access control lists (ACLS) and permissions. Update various network configuration files and established SSH keys for key-based authentication. Use RPM Package Manager to apply patches and application software.

4.12.13 Respond directly to the DMDC and other Agencies at DMDC's direction; remote military and civilian sites and other network users to resolve large-scale, networking, Linux and Enterprise computer systems hardware and software challenges.

4.12.14 Install, configure, implement and manage TCPIP and its associated servers in the z/VM environment. Coordinate TCP/IP Hardware and software configurations in the z/OS Environment, IP addresses and VPN requests with the Network Operations Center (NOC) to include in their firewall configuration. Monitor network components and resolve hardware, software and interoperability issues.

4.12.15 Plan, Install, customize and implement the Remote Spooling Communication Subsystem (RSCS) Networking system. This provides data transmission services between z/VM and z/OS.

4.12.16 Covert the z/OS Network Control Program/Systems Network Architecture/System Network Interface (NCP/SNA/SNI) network from a subarea networking environment to a SNA/TCPIP P2P Network/High Performance/Routing Enterprise Extender Network to support data transmission to the SSA network. Update and maintain VTAM z/OS and z/VM systems environments. Define Connect Direct and Cyberfusion connection within VTAM.

4.12.17 Plan, install, test, and implement backup and restore strategies using current software products. Manage, maintain and monitor its Backup and Tape environment and its associated Tape Management Catalog (TMC) and software applications scheduling products. Define procedures, standards and backup policies.

4.12.18 Install, configure, customize, implement and manage the "Data Facility Storage Management Sub-systems" (DFSMS) for Removable Media Services (RMS) for access to IBM's 3494 Automatic Tape Library (ATL) Data Server. Integrate server virtual machines and tape management

software applications to interface with RMS for backup and recovery of data. Interface and monitor the ATL environment via its Library Manager console.

4.12.19 Customize I/O hardware definitions for logical partitions (LPARS), OSA, CHIPIDS to specify channel paths installed on the Central Processor Complex (CPC) and the control units attached to these paths and the I/O devices assigned to the control units and FICON and ESCON definitions to access the manual tape drives, ATL drives and Direct Access Storage Devices (DASD).

4.13 TASK 13 – Conduct Future Projects & IT Services (Over & Above TASK)

As of P0001 – please see FASA's incorporated Technical and Pricing Proposal.

During the course of performance of the requirements identified in this PWS, it is possible that the anticipated effort could potentially expand by as much as 30% of the anticipated, on-going support hours. Offeror's are requested to utilize the 30% surge figure as a baseline in developing proposed pricing for this task, to ensure an adequate level of support is maintained. This task refers to an optional level of effort that may be exercised at the Governments discretion. The decision to invoke the task shall be based on the level of support that is required, project length and the amount of project funding received. The Government may exercise the Optional TASK more than once or in any combination thereof not to exceed 30% of the price of the current (exercised – Base or Option) performance period. The Government will provide a requirements definition for new initiatives prior to requests for support.

The contractor shall account for surge activities and provide the resources necessary to accommodate them. The resources may include an SME for program review, analysis and integration strategies. During the life of the task order the workload in any one area may grow significantly for a period of time. Some activities are recurring while others are not.

Examples of recurring activities include:

- Technology refresh cycles

Examples of non-recurring activities include:

- Major System roll outs
- Office moves
- Unexpected increases in staffing
- Implementation of new DoD programs
- Transition or transfer of existing DoD programs
- Data Center and Application Hosting Moves
- Architectural upgrades such as Active to Active Infrastructure

These activities may spur an increase in the volume of Help Desk calls or Desktop support requests. Unplanned surge activities' timing and length cannot be predicted.

Examples of expected projects and services include:

- Headquarters Reorganizations
- Migration of Services (i.e. DISS, DTS, FMTS)

4.14 Task 14- DMDC Registration Authority (OPTIONAL TASK)

The DMDC Registration Authority provides PKI activities for the DMDC Enterprise for the NIPRNET and SIPRNET environments. Services provided are SSL certificates, Domain Controller certificates, Alternate tokens, Group certificates, Code Signing certificates and SIPR tokens. PIN reset services are provided for tokens that are issued by the DMDC Registration Authority.

4.14.1 The Contractor personnel designated as the DMDC Registration Authority shall provide Registration Authority services in compliance with, but not limited to: DoD Certificate Policy, DoD PKI Certification Practice Statement, DoD NSS PKI DoD Registration Practice Statement and DoD Directives.

4.14.2 The Contractor shall designate Registration Authority (RA) officers whom are responsible for duties of certificate issuance, certificate revocation or key recovery in both the NIPRNET and SIPRNET environment. The Contractor personnel designated as the DMDC Registration Authority shall obtain their DoD PKI Registration Authority Credential and/or NSS DoD PKI Registration Authority Credential and/or JITC Registration Authority Credential. The Contractor personnel designated as the DMDC Registration Authority shall have a Secret clearance and are knowledgeable of Certificate Policies and IA concepts, practices and procedures.

4.14.3 The Contractor shall designate Local Registration Authority, Trusted Agents, System Administrators and additional RA stakeholders at various DMDC supported sites to support RA services. The Contractor will need to partner with other ITO groups, DMDC divisions or agencies to provide Registration Authority Program services.

4.14.4. The Contractor shall perform Registration Authority (RA) Program duties in a secured location during core business hours as coordination is necessary with certificate requestors.

4.14.5 The Contractor shall provide Registration Authority services in the NIPRNET and SIPRNET environment to include, but not limited to: SSL certificates, Domain Controller certificates, MultiSAN certificates, Alternate tokens, Code Signing certificates, Group Certificates and SIPR tokens. Certificate requests should be processed based upon the established DMDC Registration Authority Program Policy and SLA.

4.14.6 The Contractor shall responsible for processing certificate request through the DMDC ITO Change Management process. This includes: certificate CSR file testing, documentation verification, troubleshooting with certificate stakeholders, guiding the request through the Change Management process, certificate submission to the certificate requestor, certificate configuration item creation and documentation close out.

4.14.7 The Contractor shall responsible for the development and maintenance of RA program documentation to include, but not limited to: policies, procedures, standards, checklists, forms, NIPR/SIPR certificate tracking spreadsheets. This also includes communication and resources via SharePoint webpage. The Contractor is responsible for maintaining email groups and SharePoint access groups related to the DMDC Registration Authority Program to limit access to only required DMDC RA Program stakeholders.

4.14.8 The Contractor shall provide token services in the NIPRNET and SIPRNET environments. For the NIPRNET, token services include, but are not limited to, Alternate tokens and Code Signing tokens. For the SIPRNET, token services include, but are not limited to, SIPR tokens. Token services also include, but are not limited to, enrollment and registration of token users, maintaining token inventory, PIN resets and provide current disposition of token services.

4.14.9 The Contractor is responsible for providing reports such as: Certificate Expiration Annual Report, RA Program Quarterly Reporting, Registration Authority Team Weekly Report for ITO Senior Management, RA Program Annual Report, Ad hoc Reporting.

4.14.10 The Contractor is responsible for tracking the lifecycle of all certificates issued by the DMDC Registration Authority Program. Certificate Expiration tracking activities include, but are not limited to: annual report of certificate expirations, monthly email notifications to the DMDC Certificate Board and certificate expiration escalation.

4.14.11 The Contractor is responsible for maintaining a certificate configuration item inventory in CMDB based upon the requirements outlined in the Registration Authority Program SOP.

4.14.12 The Contractor is responsible for development and execution of training sessions for RA Program and Registration Authority program stakeholders and team members, as needed.
The Contractor is responsible for attending different meetings, developmental projects/activities and learning opportunities related to the Registration Authority community and duties.

4.14.13 The Contractor shall research and submit to the Government requests through the DMDC standardized procurement process to procure supplies, equipment, commercial certificates in support of the Registration Authority program.

4.14.14 The Contractor is responsible for executing program activities to include, but not limited to: preparing and participating in Registration Authority Program Audit by DISA.

4.14.15 The Contractor shall perform Registration Authority (RA) Program duties in a secured location during core business hours as coordination is necessary with certificate requestors.

4.14.16 The Contractor is responsible for safeguarding all RA equipment, information and property. At the close of each work period, Government facilities, equipment, and materials shall be secured.

4.14.17 The Contractor is responsible for any travel related expenses for designated Registration Authority personnel to obtain their DoD PKI Registration Authority Credential and/or NSS DoD PKI Registration Authority Credential and/or JITC Registration Authority Credential.

5.1 GENERAL REQUIREMENTS

Provide Reports, Meetings & Documentation

Reports and deliverables will be submitted in Microsoft Office products to include Microsoft Project and shall be accessible via DMDC web. All diagrams shall be delivered in a readable format (PDF or standard formats and hard copy (including oversized diagrams).

5.2 Monthly Status Report (MSR)

Submit a MSR for the previous month to the COR via email and a designated area on DMDC intranet by the 15th working day of each month. The Contractor shall prepare an agenda and meeting minutes in a clear, concise and orderly manner. Briefing materials shall be made available to all attendees prior to time of briefing. The report should include data of sufficient detail to monitor the completion of work products against progress as documented in the PWS:

- Call Order Summary
- Performance metrics
- Schedule
- Up to date Project Plan
- Milestones achieved or missed
- Open Issues/Risk and mitigation Action
- Summary of Issues Closed
- Projected Activities
- Summary of accomplishments for each project
- Issues and Risks with impact and mitigation
- Total number of server outages, duration and business impact of each outage.
- Recommended remediation for outage root cause and any contributing factors
- Report on the overall health of the system infrastructure (to include but not limited to Incident/Problem management; Event Management; Capacity Management; Project Management; Knowledge Management; Change Release Management)
- Number of help desk tickets opened and closed
- Top ten categories of Tier I, II & II support activities.
- Report on the end of life (EOL), end of support (EOS) and hardware/software
- Number of Network outages
- Statics on overall health of the infrastructure
- Application release metrics
- Database Support:
  - A list of database instances

- Servers they reside on
- Environments associated with them (PROD, TEST, etc.)
- Mainframe Status/Activity (i.e. system performance, CPU utilization, operational problems)

5.3 Communications Plan

Develop and deliver a Communications plan that provides methods, timing, roles, responsibilities and key messages. The Communication Plan will describe how the contractor will establish a reliable means of communicating status about the contract to all appropriate stakeholders. It describes what needs and how it will be communicated, who is responsible for communicating with whom and when the communication needs to take place.

The contractor will provide communications to the Director, IT Operations, Deputy Director IT Operations and the COR regarding the status of DMDC networks and service availability or degradation. Communications shall be via email and/or telephone. Reporting will include the following:

- Planned and unplanned changes or upgrades.
- Planned and unplanned system outages.
- Availability and status of networks, network services, server resources, data, systems, and peripherals.

5.4 Problem Notification Report (PNR)

The contractor shall be responsible for bringing to the attention of the COR, IT OPS Director and IT OPS Deputy Director any problems or potential problems in performing assigned tasks. Subsequent to verbal notification, a written Problem Notification Report (PNR) shall be submitted within three (3) days after identification of the problem.

5.5 Transition Plan

5.4.1 Phase In

The outgoing contractor will ensure minimal disruption to IT Operations activities and ensure a seamless transition within 30 calendar days upon contract award. The Phase-In period shall commence on the effective date of the task order and the contractor shall become operational by the end of the Phase-In period and will begin providing service to users.

During Phase-In, the current contractor and the new contractor under this task order shall:

- Conduct a joint inventory of the hardware, software and accounts
- Prepare, certify and submit a detailed Phase-In Joint Inventory Report
- Organize applications and skill sets into logical categories for migration and assimilation

- Review current operating process and procedures and make recommendations concerning lifecycle management of software, hardware and accounts management to identify opportunities for improved efficiencies and cost savings

- Review and modify escalation procedures, SOPs, and Technical Operations Manual (TOM). The incumbent contractor shall provide the most recent version of these documents to the successful Contractor as part of the transition process.

- Review existing architecture and technical infrastructure including dependencies on server/router/switch configurations, protocols, and startup parameters

- Review existing business and support processes

- Ensure all necessary security training is completed by employees during transition

5.4.2 Phase Out

The Phase-Out period may last 30 days. The contractor shall provide qualified personnel to execute Phase-Out in accordance with the COR approved Phase-Out Plan. The contractor will cooperate with the incumbent and the Government to allow for orderly turnover of equipment and documentation so as not to interfere with users' work or duties. DMDC shall retain ownership of all information tracked by all ITSS tools, including CA Unicenter, inventory tracking system and any other systems used to perform the tasks under this PWS. Thirty calendar days after the task order end date, the contractor will work with the COR to transfer this information in an approved format.

The contractor and the incumbent shall conduct a joint inventory and certify and submit a Phase-Out Joint Inventory Report for approval by the Government 15 calendar days prior to the Phase-Out end date. The inventory shall include the same data as required for the Phase-In inventory.

5.4.2.1 Technical Meetings
Participate and contribute to various agencies technical meetings to include Technical Working groups and various ad hoc technical tiger teams.

5.4.2.2 Technical Documentation
The Contractor shall document all processes developed under this PWSPWS to include systems and operations such as source and object code developed for ITSS projects, and design and specification document(s) provided to the project manager.

5.5 In-Process Project Review

Conduct in process reviews (IPRs) every other week. The Contractor shall provide the COR, IT Operations Director and IT Operations Deputy Director with a draft copy of the IPR briefing 2

business days prior to the scheduled IPR for review. At a minimum, the IPR shall report any current or anticipated projects, scheduled dates of competition, problems, resolution of existing problems, solutions implemented, and their impact, and other general project related information. The results of this task shall be documented in monthly status reports, and IPR briefing/minutes.

5.6 Conduct a Post-Award Conference

This meeting provides an introduction between the contractor personnel and Government who will be involved with the contract and will aid both parties in achieving a clear and mutual understanding of all requirements, and identify and resolve any potential issues. However, this meeting is not a substitute for the contractor fully understanding the work requirements nor is it to be used to alter the final agreement arrived at in any negotiations leading to contract award. The contractor shall be prepared to discuss any items requiring clarification and gather information as necessary to support each deliverable and shall submit a written summary of the Post-Award Conference to the COR.

5.7 After Hours Support

Non-standard business hours support shall be accessible via special access numbers or voice mail menus, with live support accessible or phone call returned within 15 minutes of initial support request. Provide the COR, Director IT Operations and Deputy Director IT Operations a roster of on call personnel and updates as changes are required.

Support personnel shall be available "on call" at the designated number, provided upon contract award, during non - standard business hours regardless of holidays or other closings. This service will be utilized in emergency situations (i.e., server room flood, power outage, widespread services outage) or other incidents reported by a user that meet emergency response criteria.

6.1 DELIVERABLES

The contractor shall provide the following deliverables and reports, the format of which will be defined and approved by the Government and subject to change over the course of the task order. All materials and information developed or produced under this task order, including but not limited to documents, presentations, recommendations and meeting minutes, are the property of the Government. The contractor shall deliver all deliverables using email to the COR, IT OPS Director and IT OPS Deputy Director.

Deliverables	PWS Reference	Date Due/Frequency
Communication Plan	4.1.1.5, 4.14.2	30 days after contract award
IT Service Catalog	4.1.2.2	180 days after contract award
Consumable Report	4.1.3.6	**4th business day of each month**
IT Inventory Report	4.1.3.9	Annually, 30 days after completion of the inventory. Initial Inventory 90

		days of contract award.
Project Management Plan	4.1.1.2 , 4.1.1.3, 4.1.1.4 ,4.10.3	Must be current within 5 business days at any time during the project
Problem Notification Report	5.3	3 days after identification of problem
Revised Event Mgmt Program Documentation/Recommended Tool	4.1.4.11	90 days after contract award
Capacity Planning Report	4.1.5.7 & 4.1.5.13	**4th business day of each month**
Release Calendar	4.1.7.11	**4th business day of each month**
Configuration Management Plan	4.1.8.26	30 days after contract award
CM Monthly Change Report	**4.1.8.29**	**4th business day of each month**
Deployment Calendar (SharePoint)	4.1.8.31	Updated Quarterly
Infrastructure upgrade report	4.1.8.32	Quarterly
COOP Failover Test Report	4.1.10.12	30 days after exercise
Disaster Recovery Plan	4.1.10.4	60 days after contract award
Technical Refresh Plan	4.1.2.7	As needed
Backup Status Report	4.3.16	Weekly
Server Disc Space Utilization Report	4.3.21	Weekly
Virtual Desktop Infrastructure Plan	4.5.18	90 days after contract award
Database Utilization Report	4.7.26	**4th business day of each month**
Monthly Status Report	**5.1**	**3 days prior to Monthly MSR Meeting**
Transition Plan (Documentation that describes the processes, procedures and controls that will be used to assure smooth transition at the end of the period of performance. To be delivered in electronic and paper form, using Microsoft Word, Excel and Power Point)	5.4	30 days prior to end of period of performance . At time of Quote Submission
Technical Documentation	5.4.2.2	As required
In-Process Review	5.5	Bi-Weekly; draft 2 business days prior to scheduled IPR
Conduct a Post award Conference	8.2	Within 5 business days after contract award
Quality Control Plan	7.1	30 days after contract award. At time of Quote Submission
Risk Management Plan	7.3	30 days after contract award

Standard Operating Procedures	4.1.9.9	90 days after contract award (review existing and update SOP's, create new SOP's identified by the Government) Every 6 months review and update as needed.
Availability Plan	4.1.6	180 days from date of award
Invoices: To be delivered in electronic and paper form, using Microsoft Word, Excel or other agreed upon form.	8.3	Monthly

6.2 Acceptance of Deliverables

The COR shall have ten (10) working days to complete review of the deliverables. The Contractor shall follow-up with the COR to ensure that the deliverables were received. The COR will reject deliverables in writing; however, acceptance may be done verbally or in writing.
If the contractor does not receive a response from the COR within 10 working days after following-up, acceptance may be assumed. In the event of the rejection of any deliverable, the Contractor shall be notified in writing by the COR or assigned representative providing specific reason(s) for the rejection. The Contractor shall have ten (10) working days to correct the rejected deliverable and return it to the GSA COR for approval.

The general quality measures, as set forth below will be applied to each deliverable received from the Contractor under this contract. These quality measures will be utilized in the QASP for the task order.

1. Accuracy - Deliverables shall be accurate in presentation, technical content, and adherence to accepted elements approved by the COR.
2. Clarity - Deliverables shall be clear and concise; All diagrams shall be clearly written and marked without ambiguity for Government team members and relevant project stakeholders.
3. Specifications Validity - All Deliverables must satisfy the requirements of the Government as specified herein and approved by the COR and, when appropriate, other Government project managers.
4. File Editing - All text and diagrammatic files shall be editable by the Government.
5. Format - Deliverables shall be submitted in hard copy (where applicable) and in media defined by the COR.
6. Timeliness - Deliverables shall be submitted on or before the due date specified by the COR or submitted in accordance with a later scheduled date as determined by the COR. Softcopies of reports shall be submitted electronically to the COR electronic e-mail address. In the event the system is unavailable or not accessible due to a system

malfunction, the Contractor shall submit all reports in a typewritten format to be followed simultaneously with an electronically transmitted copy as soon as the electronic mail system becomes available.

7.1 QUALITY MANAGEMENT

7.2 Quality Control Plan (QCP)

The Contractor shall develop and maintain an effective quality control program to ensure services are performed in accordance with this PWS. The contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of sub-standard services. The quality control program is the means by which he assures himself that his work complies with the requirement of the contract. The Quality Control Plan (QCP) shall be provided 30 days after award. A copy of the comprehensive written QCP shall be submitted to the Contracting Officer (KO) and COR within 5 working days when changes are made thereafter. After acceptance of the quality control plan the contractor will receive the Contracting Officer's acceptance in writing of any proposed changes.

7.3 Quality Assurance Surveillance Plan

7.3.1 The Government reserves the right to perform inspections and surveillance to evaluate the contractor’s compliance to the contract terms and performance of the requirements in the PWS. The Government will make every effort to ensure that the surveillance methods described below are conducted in an objective, fair, and consistent manner.

1. Periodic Surveillance. This action occurs when the COR or other Government official observes a deficiency. Examples include evidence from accidents, incidents, or delays. Regardless of where in the line-of-duty the COR observes contractual procedures not being followed, he/she has an obligation to document and report the deficiency to the Contracting Officer.

2. Customer Complaint Surveillance. This action is instituted when the COR receives a complaint from a stakeholder regarding Contractor service. The COR will obtain the complaint in writing and then conduct an investigation to determine its validity. If the complaint is deemed valid, the COR will immediately notify the contracting Officer for action. The COR will notify both the Contract Manager and the complainant of the Government’s response to their complaint.

7.3.2 Contract Discrepancy Report (CDR). In the event of unsatisfactory contractor performance, the COR or KO will issue a CDR that will explain the circumstances and findings concerning the incomplete or unsatisfactory service. The contractor will acknowledge receipt of the CDR and respond in writing as to how he/she shall correct the unacceptable performance and avoid a recurrence. The Government will review the corrective action response to determine acceptability

and will use any completed CDR as part of an overall evaluation of Contractor performance when determining present or future contractual actions.

7.4 Risk Management Plan (RMP)

The contractor shall employ a comprehensive and proven risk management approach and employ a formal Risk Management Plan (RMP) that details (a) a routine and regular process involving both the contractor and the Government program staff to identify, analyze, prioritize and detail appropriate and agreed upon responses to the highest priority risks and (b) the work products that result from performance of the process. Establish, update, and implement a Risk Management Plan with an organized, systematic decision making process, including the criteria, methods, and procedures for effectively managing risks related to this contract.

8.1 Additional Requirements

8.2 Telework

The Government may permit from time-to-time telecommuting by contractor employees when determined to be in the best interest of the Government in meeting work requirements. The contractor must have an established program and provide adequate oversight of work products to ensure contract adherence. All telecommuting agreements must be authorized and approved by the COR and include the date, time, and description of the tasks to be performed. Telework capability must be demonstrated at the time of telework request. Telecommuting will be at no additional cost to the Government.

8.3 Post- Award Conference / Kick-Off Meeting

The Contractor shall attend any post award conference convened by the contracting activity or contract administration office in accordance with Federal Acquisition Regulation Subpart 42.5. The CO, COR, and other Government personnel, as appropriate, may meet periodically with the contractor to review the contractor's performance. At these meetings the Contracting Officer Representative will apprise the contractor of how the Government views the contractor's performance and the contractor will apprise the Government of problems, if any, being experienced. Appropriate action shall be taken to resolve outstanding issues.

All contractor personnel assigned to this Task Order must be cleared through a National Agency Check and Inquiry (NACI) background check and provide documentation before providing services or beginning work under this Task Order. The contractor shall submit security paperwork at the Post-Award Conference/ Kick-Off Meeting in order to prevent delay in task order performance.

8.4 Invoice and Payment

Invoices and supporting documentation shall be submitted to the COR for review prior to submission to the GSA Office of Finance. Additionally, original invoices shall be submitted to the

GSA Office of Finance. Supporting documentation shall include all information necessary to verify charges (e.g. timesheets).

Addresses for the GSA Finance Office and the COR will be provided at award.
Invoices shall include—

- Name and address of the Contractor;
- Invoice date and number;
- Contract number and contract line item number;
- Description, quantity, unit of measure, unit price and extended price of the items delivered. The information should be separated by each subtask as outlined in section 4.1 through 4.5;
    - Labor hours should be specific for each contractor and associated labor category;
- Terms of any discount for prompt payment offered;
- Name and address of official to whom payment is to be sent;
- Name, title, and phone number of person to notify in event of defective invoice;
- Taxpayer Identification Number (TIN). The Contractor shall include its TIN on the invoice only if required elsewhere in this contract; and
- Electronic funds transfer (EFT) banking information as follows
    - (A) The Contractor shall include EFT banking information on the invoice only if required elsewhere in this contract.
    - (B) If EFT banking information is not required to be on the invoice, in order for the invoice to be a proper invoice, the Contractor shall have submitted correct EFT banking information in accordance with the applicable solicitation provision, contract clause (e.g., 52.232-33, Payment by Electronic Funds Transfer—Central Contractor Registration, or 52.232-34, Payment by Electronic Funds Transfer—Other Than Central Contractor Registration), or applicable agency procedures.
    - (C) EFT banking information is not required if the Government waived the requirement to pay by EFT.
- Any submitted invoice(s) must match the information currently found within the System for Award Management (SAM) website. Contractors are encouraged to verify their current registration information at https://www.sam.gov prior to preparing and submitting invoices to avoid unnecessary invoice processing delays or invoice rejects.

8.5 Identification of Contract Employees

All contract personnel attending meetings, answering Government telephones, sending or receiving emails and working in other situations where their contractor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression in the minds of members of the public that they are Government officials. They must also ensure that all documents or reports produced by contractors are suitably marked as contractor products or that contractor participation is appropriately disclosed. Provisions of the Privacy Act apply to all records and reports maintained by the contractor.

8.6 Contractor Capacity

The Contractor is required to perform the requirements of this PWS by providing a sufficient level of personnel resources to assure uninterrupted support for all task areas for the duration of this task order. GSA expects this level of support will be maintained at the level proposed in the quotation response throughout the entire period of performance of this Task Order and exercised options. GSA expects Contractor Personnel with the appropriate skills will be provided throughout the performance period of this Task Order. If Offeror fails to maintain the quoted level of Workforce Capacity to meet task order requirements, the Contracting Officer, by written notice, may terminate this contract, in whole or in part, when it is in the Government's interest. If this contract is terminated, the Government may exercise its full right to any and all remedies. "contractor personnel". Contractor must maintain the mix of staff as proposed for the overall contract effort which should be detailed in the staffing matrix/cost proposal. Appendix C indicates "extensive experience and knowledge is required but not limited to the items listed:"

8.7 Government Use of Data

The Government requires unlimited rights in any material first produced in the performance of this task order, in accordance with the FAR clause at 52.227-14 and 52.227-16. In addition, for any material first produced in the performance of this task order, the materials may be shared with other agencies or Contractors during the period of performance of this task order, or after its termination. For any sub-contractor or teaming partners, the contractor shall ensure at proposal submission that the sub-contractor and /or teaming partners are willing to provide the data rights required under this task order. The Government intends to use this information on future Government requirements. Reference: DFAR clause (252.227-7014) Rights in Non-commercial Computer software and noncommercial computer software documentation and (252.227-7013) Rights in Technical Data--Noncommercial Items.

8.8 Organizational Conflict of Interest

If the contractor is currently providing support or anticipates providing support that creates or represents an actual or potential organizational conflict of interest (OCI), they will immediately disclose this actual or potential OCI in accordance with FAR Part Subpart 9.5. The contractor is also required to complete and sign an Organizational Conflict of Interest Statement in which the Contractor (and any sub-contractors, consultants or teaming partners) agree to disclose information concerning the actual or potential conflict with any proposal for any solicitation relating to any work in the contract. All actual or potential OCI situations shall be handled in accordance with FAR Subpart 9.5.

8.9 Non-Disclosure Requirements

All Contractor personnel (to include sub-contractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the contract issued which requires

the contractor to act on behalf of, or provide advice with respect to any phase of an agency procurement, as defined in FAR 3.104-4, shall execute and submit an "Employee/Contractor Non-Disclosure Agreement" Form. This is required prior to the commencement of any work on the contract and whenever replacement personnel are proposed under an ongoing contract. Any information obtained or provided in the performance of this work is only to be used in the performance of the contract.

8.10 508 Compliance

The contractor shall support the Government in its compliance with Section 508 through-out the development and implementation of the work to be performed. Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d) requires that when Federal agencies develop, procure, maintain, or use electronic information technology, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who do not have disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency.

Section 508 also requires that individuals with disabilities who are members of the public seeking information or services from the Federal Agency, have access to and use of information and data that is comparable to that provided to the pubic who are not individuals with disabilities, unless an undue burden would be imposed on the agency.

The Offer should review the following websites for additional 508 compliance information.

http://www.section508.gov/index.cfm?FuseAction=Content&id=12
http://www.access-board.gov/508.htm
http://www.w3.org/WAI/Resources

9.1 TRAVEL

Local or long-distance travel may be required to various locations, as directed by the Government, in order to perform the tasks delineated in this PWS. Reimbursement of travel expenses are limited to those expenses incurred by the contractor's employees in a COR approved travel status only. The contractor is not authorized to make travel arrangements or incur expenses on behalf of Federal employees, military or civilian, during performance of this contract. Requests for reimbursement of these unauthorized expenditures shall be rejected.

Travel requests: All travel including local travel, if authorized, shall be approved by the COR prior to commencement of travel. When requesting approval by the COR, the contractor shall submit the following information to the COR in writing:

- Name(s) of traveler(s)
- Dates of travel
- Purpose of travel
- Travel itinerary (include all locations where duties will be performed by the traveler or there will be overnight stays)
- Whether a rental car will be required
- Identify any special requirements with justification of the traveler (e.g. requirement for a mid-size rental car; medical justification for other than economy class airfare)
- Estimated cost (breakdown via airfare, lodging, rental car, mileage, meals & incidentals, parking, etc.) with total cost

Travel expenses will be reimbursed to the contractor in accordance with FAR 31.205-46, the Contractor Travel (Feb 2013) clause and the instructions contained within this section upon submission of proper documentation with the contractor's invoice.

10.0 GOVERNMENT FURNISHED EQUIPMENT (GFE)

The Government will furnish office space which will include desk, telephone, and computers along with access to office applications necessary to conduct business for on-site contractor personnel. The Government shall provide access to Government owned software and all hardware procured will become Government Furnished Equipment (GFE). The contractor shall safeguard all Government Furnished Property (GFP), equipment, software, and information. Additionally, for the off-site pricing scenario, the contractor should assume it will be responsible for providing all resources including all personnel, equipment, supplies, facilities, transportation, tools, materials, supervision, and other items necessary to provide the non-personal services detailed herein at the contractor facility. At the request of the Government, or at completion of this effort, the Contractor shall immediately return any Government-provided property, including any equipment, specialized or off-the-shelf software, and all other property provided by the Government for the Contractor to use to complete this effort.

11.0 PLACE OF PERFORMANCE

DMDC anticipates the majority of work performed under this task will be by on-site personnel. However, the contractor shall propose both on-site and off-site staff for consideration. Places of performance can be found in Appendices. Places of performance may vary, at the Government's sole discretion and direction, during performance as required to meet Government requirements. The contractor may be required to house integrated project/program teams at their facility in the future.

12.0 PERSONAL SERVICE

The client has determined that use of the GSA contract to satisfy this requirement is in the best interest of the Government, economic and other factors considered, and this task order is not being

used to procure personal services prohibited by the Federal Acquisition Regulation (FAR) Part 37.104 titled "Personal services contract".

13.0 KEY PERSONNEL

The Contractor shall provide the Government with a list of proposed staff to meet the key personnel requirements of this PWS, and the resumes for each. The Government will have final determination on the qualifications of identified personnel. Throughout the course of the contract, if key personnel are replaced, the Contractor must receive approval from the Government on the resume of the intended replacement prior to that individual being utilized for this contract. No Key Personnel substitutions will be allowed during the first 90 days of the Contract unless caused by an individual's death, disability or termination.

Key personnel proposed and accepted for this contract are expected to remain dedicated to this contract. During the performance period from contract initiation until completion no key personnel substitutions will be permitted unless such substitutions are necessitated by an individual's sudden illness, death, termination of employment or as otherwise approved by the Contracting Officer (CO). In any of these events the Contractor must promptly notify the CO. Prior to changing any of the specified key personnel individuals to other programs for whatever reason, the Contractor shall notify the CO reasonably in advance, preferably more than 30 days, and shall submit a detailed explanation of the circumstance necessitating the proposed substitutions, a complete resume for each proposed substitute and any other information requested by the CO, to permit evaluation of the impact on the program. The CO will evaluate such requests and promptly notify the Contractor whether the proposed substitution has been approved or disapproved. No diversion shall be made by the Contractor without the written consent of the CO, provided, that the CO may confirm in writing such diversion and such confirmation shall constitute the consent of the CO dictated by this clause. As appropriate, the list of key personnel may be modified during the period of performance of the contract to either add or delete personnel.

The Contractor agrees to assign to the contract: persons who are necessary to fill the requirements of the contract, whose resumes are submitted with its quote, and who are specifically defined as key personnel. No substitutions shall be made except in accordance with the PWS.
The Government shall have final determination on the qualifications of identified personnel. The Government expects that at a minimum, eighty percent (80%) of Key Personnel will show up on the first day of the contract performance.

The Contractor shall assign to this contract the following Key Personnel:

Program Manager
ITSM Lead
Incident Manager Lead
Lead Project Manager

14.1 SECURITY

The Government requires the contractor to establish that applicants or incumbents either employed by the Government or working for the Government under this contract are suitable for the job and are eligible for a Common Access Card (CAC) and public trust position at the appropriate level or security clearance prior to contract award date. This includes the following:

14.2 Security Clearance Requirements

Contractor personnel must be able to obtain and maintain the requiring access to classified information will need to obtain the appropriate security clearance prior to beginning work on this contract.

14.2.1 DMDC is not responsible for processing Contractor personnel for national security clearance (SECRET).

14.2.2 The contractor must comply with required DMDC personnel security requirements as specified by the Cybersecurity Branch.

14.2.3 Interim Clearances will be reviewed upon notification to DMDC Information Security Branch.

14.2.4 It is the responsibility of the contractor FSO to notify DMDC immediately if there is a change in clearance eligibility.

14.2.5 If at any time, any contractor FSO is unable to obtain/maintain an adjudicated Personnel Security Investigation (PSI), the Contractor shall immediately notify the DMDC Cybersecurity Branch and remove such person from work under this contract.

14.3 CAC Requirements

Contractor personnel with access to DMDC systems or data must comply with HSPD-12 Personal Identity Verification (PIV) issuance requirements, known as the Common Access Card (CAC) for DMDC and must be CAC or PIV ready prior to beginning work on this contract:

14.3.1 All Contractor personnel must obtain/maintain a favorable FBI National Criminal History Check (fingerprint check).

14.3.2 Provide two forms of identity proofed identification (I-9 documents).

14.3.3 Be citizens of the United States.

14.3.4 Submit a Standard Form (SF) 86 National Security Questionnaire through e-QIP that is favorably accepted by the Office of Personnel Management (OPM) for those:

- Who do NOT have an active security clearance
- Will be obtaining a position of trust through DMDC or
- Have NOT been favorably adjudicated within the last 24 months.

14.3.5 Schedule a Background investigation by OPM.

14.3.6 Maintain favorable FBI National Criminal History checks and ensure completion and successful adjudication as required for Federal employment.

14.3.7 Obtaining CAC or PIV ready status is the responsibility of the Contractor. It is the responsibility of the Contractor to notify DMDC when this is complete.

14.4 Position of Trust Requirements

14.4.1 All Contractor personnel with access to DMDC systems or data must comply with DODI 5200.2-R and DODI 8500.1. All persons on this contract will be designated as either an IT-I or IT-II as determined by the Government per position responsibilities. All enterprise wide system administration support, to include the mainframe support services will require IT-I.

14.4.2 Prior to beginning work on this contract, the Contractor will complete all required DMDC personnel security requirements as specified by the Cybersecurity Branch.

14.4.3 Submit a Standard Form (SF) 86 National Security Questionnaire through e-QIP that is favorably accepted by the Office of Personnel Management (OPM) for all employees under this contract requesting a position of trust.

14.4.4 It is the responsibility on the Contractor to ensure their employees and sub-Contractor s (if applicable) comply with DMDC personnel security requirements.

14.5 LAN Access Requirements:

It is the responsibility of the Contractor to comply with account access requirements as specified by the DMDC Cybersecurity Branch. At minimum:

- Completed DMDC personnel security requirements.
- Complete DD 2875 Form(s) for all access required.
- Submit proof of completion for Personally Identifiable Information (PII) Training.
- Submit proof of completion Information Assurance/Cyber Awareness Challenge Training.
- Adhere to and sign the DMDC Information Systems User Agreement(s).

14.6 Information Assurance Requirements:

The Contractor and all Contractor personnel with access to or responsibility for nonpublic Government data under this contract shall comply with DoD Directive 8500.1 Cybersecurity, , DODI 8510.01 Risk Management Framework, NIST 800-53, DoD Directive 5400.11 DoD Privacy Program, DoD 6025.18-R DoD Health Information Privacy Regulation, DoD 5200.2-R Personnel Security Program, and Homeland Security Presidential Directive (HSPD) 12.

14.5.1 The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all nonpublic Government data to ensure the confidentiality, integrity, and availability of Government data. At a minimum, this must include compliance with DoDD 8500.01 and DoDI 8510.01 and provisions for personnel security and the protection of sensitive information, including Personally Identifiable Information (PII).

14.5.2 Contractor systems and information networks that receive, transmit, store, or process nonpublic Government data must be accredited according to DoDI 8510.01 Risk Management Framework and comply with annual Federal Information Security Management Act (FISMA) security control testing. All systems subject to RMF must present evidence of Assessment and Accreditation (A&A). Evidence of FISMA compliance must be presented in the form of a POA&M. The Contractor will be responsible for the cost of IA A&A and FISMA testing required for any Contractor owned and operated network, facility and/or application processing DoD information.

14.5.3 The Contractor shall ensure all media containing sensitive information (e.g., hard drives, removable disk drives, CDs, DVDs) considered for disposal will be destroyed. Prior to destruction, media will be sanitized, i.e., all prudent and necessary measures shall be taken to ensure data cannot be retrieved through known conventional or unconventional means.
To the extent that the work under this contract requires the Contractor to have access to DoD sensitive information the Contractor shall after receipt thereof, treat such information as confidential and safeguard such information from unauthorized use and disclosure. The Contractor agrees not to appropriate such information for its own use or to disclose such information to third parties unless specifically authorized by the Government in writing.

14.5.4 The Contractor shall allow access only to those employees who need the sensitive information to perform services under this contract and agrees that sensitive information shall be used solely for the purpose of performing services under this contract. The Contractor shall ensure that its employees will not discuss, divulge or disclose any such sensitive information to any person or entity except those persons within the organization directly concerned with the performance of the contract.

14.5.5 Contractor shall administer a monitoring process to ensure compliance with DoD Privacy Programs. Any discrepancies or issues should be discussed immediately with the COR and corrective actions will be implemented immediately.

14.5.6 The contractor will report immediately to the DMDC CIO / Privacy Office and secondly to the COR discovery of any Privacy breach. Protected PII is an individual's first name or first initial and last name in combination with any one or more of the following data elements: social security number; biometrics; date and place of birth; mother's maiden name; criminal, medical and financial records; educational transcripts, etc.

Government may terminate this contract for default if Contractor or an employee of the Contractor fails to comply with the provisions of this clause. The Government may also exercise any other rights and remedies provided by law or this contract, including criminal and civil penalties.

14.5.7 The Contractor is responsible for safeguarding all Government equipment, information and property. At the close of each work period, Government facilities, equipment, and materials shall be secured.

14.6 Classified Data Processing.
Based on DoD Regulation 5200.2-R, some aspects of the tasking described in this PWS requires, at minimum, a SECRET Clearance, or a SECRET Clearance In Progress, for employees who support the classified systems and/or applications at DMDC. All documentation and cost for clearance processing shall be the responsibility of the contractor. Upon award, a DD Form 254 will be issued to the contractor. All classified data processing must be completed in an approved classified processing facility. Approved classified processing facilities include: DMDC, Seaside, CA, and the Mark Center, Alexandria, VA. Additional classified processing facilities may be identified within specific tasks.

15.0 APPENDICES

Appendix A - Acceptable Quality Levels (AQLs)/ Service Level Agreements (SLAs)
Appendix B - Standard Operating Procedures
Appendix C - Experience and Knowledge
Appendix D - DMDC Locations and Users
Appendix E - Current Projects List and Backlog Intake
Appendix F - Asset Inventory:
    Incorporates the following:
    Appendix O – Printer Support
    Appendix P – Mainframe Hardware/Software
Appendix G - Major Incident, Problem Management
Appendix H - Capacity Management
Appendix I - Change Management
Appendix J - CM Historical Workload
Appendix K - Knowledge Management
Appendix L - Disaster Recovery
Appendix M - Network & Telecom Infrastructure
Appendix N - Helpdesk Historical Workload
~~Appendix O – Printer Support~~
~~Appendix P – Mainframe Hardware/Software~~
Appendix Q – ITO Workload Trends
Appendix R - Information Management Systems (IMS)
Appendix S - DD254
Appendix T - DMDC Registration Authority Workload
Appendix U - Future Program List
Appendix V - Team Quest (monitored items, ITSAR, statistics, storage VMWare dashboard)

16.0 ATTACHMENTS

Attachment 1: Contractor Employee, Agent or Representative Nondisclosure Statement
Attachment 2: Quality Assurance Surveillance Plan
Attachment 3: Price Schedule: List of Supplies and/or Services Template
Attachment 4: Past Performance Questionnaire